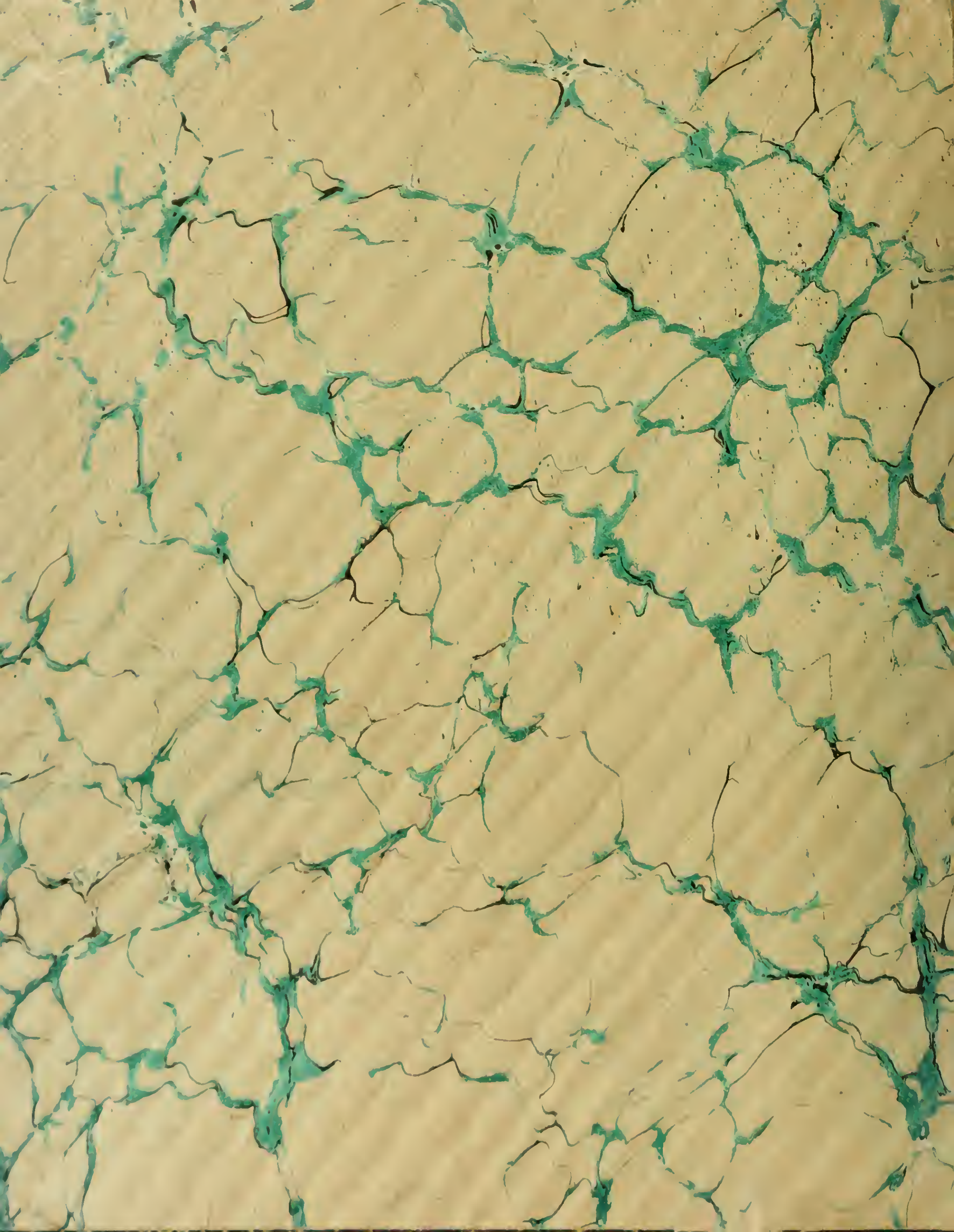
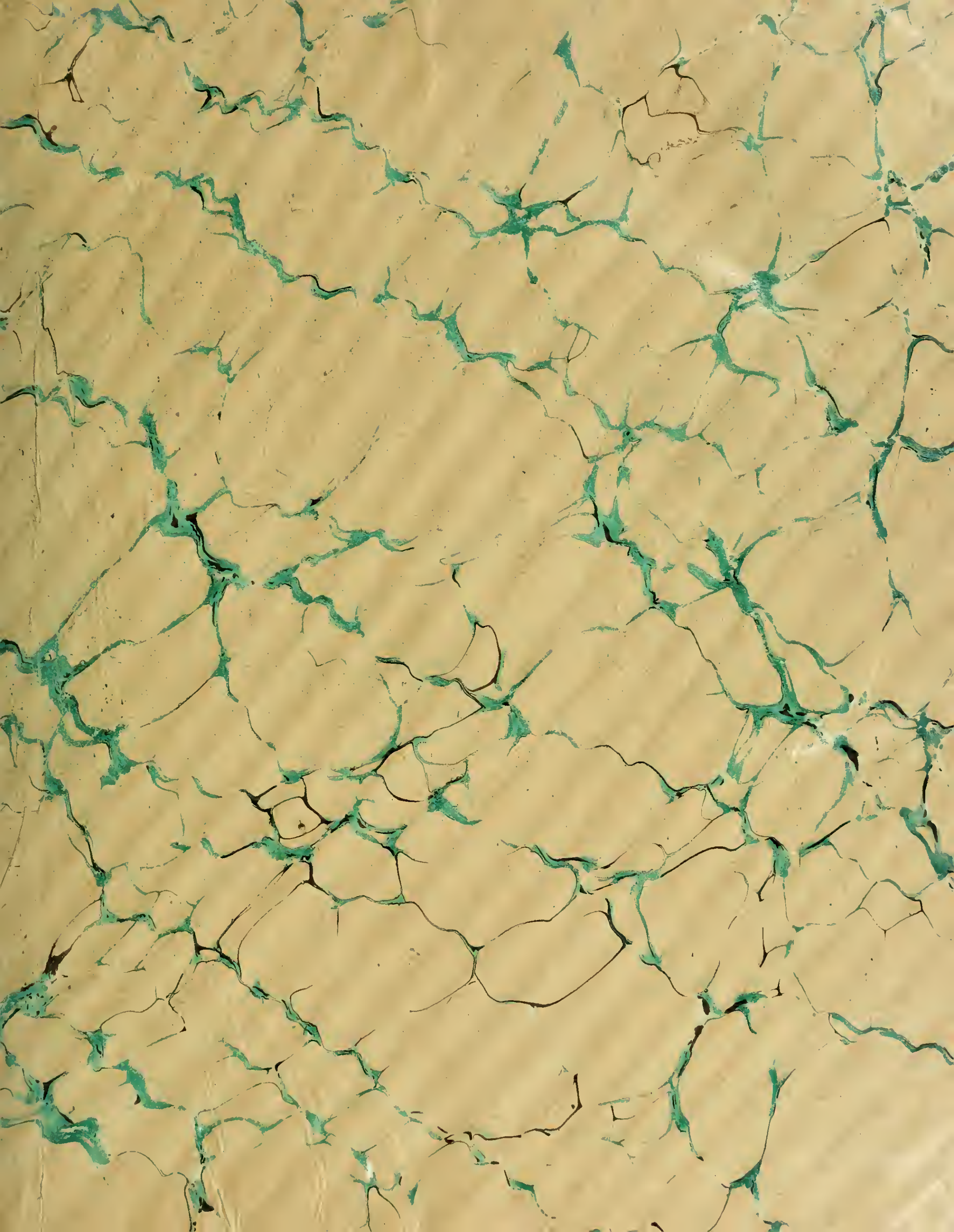




# JOURNAL

DE

# MATHÉMATIQUES

PURES ET APPLIQUÉES.

PARIS. — IMPRIMERIE DE MALLET-BACHELIER
rue de Seine-Saint-Germain, 10, près l'Institut.

# JOURNAL

DE

# MATHÉMATIQUES

## PURES ET APPLIQUÉES,

OU

## RECUEIL MENSUEL

DE MÉMOIRES SUR LES DIVERSES PARTIES DES MATHÉMATIQUES;

Publié

PAR JOSEPH LIOUVILLE,

MEMBRE DE L'ACADÉMIE DES SCIENCES ET DU BUREAU DES LONGITUDES,
PROFESSEUR AU COLLÉGE DE FRANCE.

**DEUXIÈME SÉRIE. — TOME VI. — ANNÉE 1861.**

PARIS,
MALLET-BACHELIER, IMPRIMEUR-LIBRAIRE
DE L'ÉCOLE POLYTECHNIQUE ET DU BUREAU DES LONGITUDES,
Quai des Augustins, n° 55.

1861

Digitized by the Internet Archive
in 2010 with funding from
University of Ottawa

http://www.archive.org/details/s2journaldemat06liou

# TABLE DES MATIÈRES.

## DEUXIÈME SÉRIE. — TOME VI.

# ERRATA.

---

Page 98, ligne 11, *au lieu de* $4\nu + 1$, *lisez* $8\nu + 5$.
Page 99, ligne 19, *au lieu de* $4\nu + 1$, *lisez* $8\nu + 5$.
Page 228, ligne 6, *au lieu de* $B(2^\alpha a) = B(2^{\alpha-1} n)$, *lisez* $B(2^\alpha m) = B(2^{\alpha-1} m)$.
Page 231, ligne 12, *au lieu de* points, *lisez* plans
Page 235, ligne 18, *au lieu de* $\zeta_0(n)$ et $\rho_0(n)$, *lisez* $\zeta_0(m)$ et $\rho_0(m)$.
Page 373, ligne 15, *avant* C'est là, *mettez* Ajoutons que $Z_\mu(1)$ et $R_\mu(1) = 1$.

JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES.

# THÉORÈMES

CONCERNANT

LE QUADRUPLE D'UN NOMBRE PREMIER CONTENU DANS L'UNE OU DANS L'AUTRE DES DEUX FORMES $8\mu+3$, $8\mu+5$;

PAR M. J. LIOUVILLE.

Le quadruple ($4m$) d'un nombre premier donné $m$, de l'une ou de l'autre des deux formes linéaires $8\mu+3$, $8\mu+5$, jouit de propriétés curieuses.

1° On peut poser au moins une fois (et toujours un nombre impair de fois) l'équation

$$4m = (8t+1)^2 + p^{4l+1}y^2,$$

$t$ étant un entier indifféremment positif, nul ou négatif, d'ailleurs pair ou impair, tandis que $y$ est impair et positif; quant à $p$, c'est un nombre premier ($8\nu+3$) qui ne divise pas $y$ : on admet pour $l$ la valeur zéro.

L'expression $(8t+1)^2$, en y prenant $t$ positif, nul ou négatif, donne les carrés des nombres positifs de ces deux formes

$$8s+1, \quad 8s-1,$$

savoir

$$1^2,\ 7^2,\ 9^2,\ 15^2,\ 17^2,\ldots;$$

notre théorème revient donc à dire qu'il y a un nombre impair des termes de la suite

$$4m-1^2,\ 4m-7^2,\ 4m-9^2,\ 4m-15^2,\ 4m-17^2,\ldots,$$

qu'on peut exprimer par

$$p^{4l+1}y^2,$$

$p$ étant un nombre premier non diviseur de $y$ et naturellement de la forme $8\nu+3$.

2° On peut de même poser au moins une fois (et toujours un nombre impair de fois) l'équation

$$4m=(8t+3)^2+p^{4l+1}y^2,$$

$t$ continuant à être un entier indifféremment positif, nul ou négatif, $y$ un entier positif impair, et $p$ un nombre premier $(8\nu+3)$ qui ne divise pas $y$.

L'expression $(8t+3)^2$, en y prenant $t$ positif, nul ou négatif, donne les carrés des nombres positifs de ces deux formes

$$8s+3,\quad 8s-3,$$

savoir

$$3^2,\ 5^2,\ 11^2,\ 13^2,\ 19^2,\ldots;$$

notre second théorème revient donc à dire qu'il y a un nombre impair des termes de la suite

$$4m-3^2,\ 4m-5^2,\ 4m-11^2,\ 4m-13^2,\ 4m-19^2,\ldots,$$

qu'on peut exprimer par

$$p^{4l+1}y^2,$$

$p$ étant un nombre premier non diviseur de $y$ et naturellement de la forme $8\nu+3$.

Si, au lieu de considérer séparément les deux équations

$$4m = (8t+1)^2 + p^{4l+1}y^2$$

et

$$4m = (8t+3)^2 + p^{4l+1}y^2,$$

on avait voulu considérer l'équation unique

$$4m = x^2 + p^{4l+1}y^2,$$

qui les renferme toutes deux en conservant à $y$ et à $p$ leur signification et en prenant pour $x$ un entier impair (positif) quelconque, le nombre N des solutions de cette équation unique aurait été pair; et nos méthodes, en nous indiquant ce fait de $N \equiv 0 \pmod{2}$, n'auraient pas pu nous faire savoir que l'on n'a jamais $N = 0$. Au contraire, en décomposant l'équation

$$4m = x^2 + p^{4l+1}y^2$$

en deux autres, eu égard à la valeur de $x$ (mod. 8), nous décomposons aussi N en deux parties $N_1$, $N_2$ sur lesquelles nos méthodes ont prise. Réussissant alors à reconnaître que $N_1$ et $N_2$ sont des entiers impairs, nous pouvons en conclure que N est essentiellement $> 0$. Il fallait séparer deux groupes de nombres, que l'équation unique mêlait mal à propos, pour obtenir des résultats précis.

Les théorèmes que nous venons d'énoncer au sujet des nombres $N_1$ et $N_2$ sont aisés à établir. Mais nous nous bornerons ici à les vérifier numériquement sur les exemples les plus simples.

Commençons par les nombres premiers $m$ de la forme

$$8\mu + 3.$$

Le plus petit est 3; or on a d'une part

$$4.3 = 1^2 + 11.1^2,$$

et d'autre part

$$4.3 = 3^2 + 3.1^2,$$

conformément à nos deux théorèmes. Vient ensuite $m = 11$, pour le-

quel on trouve

$$4.11 = 1^2 + 43.1^2$$

et

$$4.11 = 5^2 + 19.1^2.$$

Une vérification semblable a lieu pour $m = 19$, en vertu des équation s canoniques

$$4.19 = 1^2 + 3.5^2$$

et

$$4.19 = 3^2 + 67.1^2;$$

l'équation

$$4.19 = 7^2 + 3^3.1^2$$

ne doit pas être comptée ici, parce que l'exposant 3 n'est pas de la forme $4l + 1$.

En faisant encore

$$m = 43,$$

on a, d'un côté, l'équation canonique

$$4.43 = 1^2 + 19.3^2,$$

et, d'une autre part, ces trois-ci :

$$4.43 = 3^2 + 163.1^2,$$
$$4.43 = 5^2 + 3.7^2,$$
$$4.43 = 13^2 + 3.1^2.$$

Toujours nos théorèmes sont vérifiés : arrêtons-nous donc (quant à la forme $8\mu + 3$) au dernier exemple de

$$m = 59,$$

pour lequel les équations voulues sont

$$4.59 = 15^2 + 11.1^2$$

et

$$4.59 = 3^2 + 227.1^2,$$
$$4.59 = 5^2 + 211.1^2,$$
$$4.59 = 13^2 + 67.1^2.$$

Passons aux nombres premiers $m$ de la forme

$$8\mu + 5.$$

Le plus petit de ces nombres est 5; or on a, d'une part,

$$4.5 = 1^2 + 19.1^2$$

et, d'autre part,

$$4.5 = 3^2 + 11.1^2,$$

conformément à nos deux théorèmes. Vient ensuite $m = 13$, pour lequel on trouve

$$4.13 = 7^2 + 3.1^2$$

et

$$4.13 = 3^2 + 43.1^2;$$

l'équation

$$4.13 = 5^2 + 3^3.1^2$$

ne doit pas être comptée ici parce que l'exposant 3 n'est pas de la forme $4l + 1$. Nos théorèmes sont également vérifiés pour $m = 29$, en vertu des équations canoniques

$$4.29 = 7^2 + 67.1^2$$

et

$$4.29 = 3^2 + 107.1^2.$$

Soit encore

$$m = 37:$$

on aura semblablement les équations de forme voulue

$$4.37 = 1^2 + 3.7^2,$$
$$4.37 = 7^2 + 11.3^2,$$
$$4.37 = 9^2 + 67.1^2,$$

et

$$4.37 = 3^2 + 139.1^2;$$

l'équation

$$4.37 = 11^2 + 3^3.1^2$$

a dû être mise de côté par la raison déjà donnée plus haut que l'exposant 3 n'est pas de la forme $4l+1$.

Enfin, soit

$$m = 53:$$

il viendra les équations canoniques

$$4.53 = 1^2 + 211.1^2,$$
$$4.53 = 7^2 + 163.1^2,$$
$$4.53 = 9^2 + 131.1^2,$$

et

$$4.53 = 13^2 + 43.1^2.$$

Dans cet exemple, comme dans ceux qui précèdent et dans tous ceux qu'on pourrait ajouter, nos deux théorèmes ont lieu.

# THÉORÈME

## CONCERNANT LES NOMBRES PREMIERS DE LA FORME $16k+13$;

PAR M. J. LIOUVILLE.

Le théorème que je veux donner ici, au sujet des nombres premiers de la forme $16k+13$, consiste en ce que si l'on prend à volonté un tel nombre $m$, on pourra toujours poser un nombre impair de fois l'équation

$$m = 2^{\alpha+3}x^2 + p^{4\beta+1}y^2,$$

$x$ et $y$ étant des entiers impairs (positifs) et $p$ un nombre premier $8g+5$ qui ne divise pas $y$ : on admet pour $\alpha$ et pour $\beta$ la valeur zéro.

Le produit $2^{\alpha+3}x^2$, en y prenant successivement $\alpha = 0, 1, 2, 3,\ldots$ fournit les séries suivantes :

$$\begin{array}{llll} 8.1^2, & 8.3^2, & 8.5^2, & 8,7^2,\ldots, \\ 16.1^2, & 16.3^2, & 16.5^2, & 16.7^2,\ldots, \\ 32.1^2, & 32.3^2, & 32.5^2, & 32.7^2,\ldots, \\ 64.1^2, & 64.3^2, & 64.5^2, & 64.7^2,\ldots, \\ \ldots & \ldots & \ldots & \ldots \end{array}$$

Notre théorème revient donc à dire que si du nombre premier donné $m$, de la forme $16k+13$, on retranche ceux des termes de ces séries dont la grandeur est moindre, il y aura un nombre impair de restes qui s'exprimeront par

$$p^{4\beta+1}y^2,$$

$p$ étant un nombre premier non diviseur de $y$ et naturellement de la forme $8g+5$.

Ce théorème se vérifie d'abord pour $m = 13$ et pour $m = 29$ : on a, en effet, les équations de la forme voulue

$$13 = 8.1^2 + 5.1^2$$

et

$$29 = 16.1^2 + 13.1^2.$$

Il a également lieu pour $m = 61$ ; mais alors on trouve trois équations canoniques :

$$61 = 8.1^2 + 53.1^2,$$
$$61 = 16.1^2 + 5.3^2,$$
$$61 = 32.1^2 + 29.1^2.$$

On en rencontre également trois pour $m = 109$, savoir

$$109 = 8.1^2 + 101.1^2,$$
$$109 = 8.3^2 + 37.1^2,$$
$$109 = 64.1^2 + 5.3^2.$$

Il serait inutile de pousser plus loin les exemples.

DE

# QUELQUES PROPOSITIONS RÉCIPROQUES

RELATIVES

## A LA THÉORIE DES COURBES ET DES SURFACES DU SECOND DEGRÉ;

PAR M. PAUL SERRET.

---

I.

1. THÉORÈME I. — *Si* tout *système de cordes parallèles d'une courbe plane admet un diamètre rectiligne, cette courbe est du second degré* (Bertrand).

La démonstration la plus simple de ce théorème repose sur l'emploi de la proposition *directe*. On peut cependant éviter cet emploi, si on le veut, et trouver, à priori, l'équation différentielle de la courbe.

Nous remarquerons d'abord, à cet effet, que si une corde $mm'$ d'une courbe quelconque fait partie d'un système de cordes parallèles admettant un diamètre rectiligne, l'on a, pour le rapport des rayons de courbure aux extrémités de cette corde,

$$(1) \qquad \frac{\rho}{\rho'} = \left(\frac{mt}{m't}\right)^3,$$

$mt$, $m't$ étant les longueurs des tangentes, menées par les extrémités de la corde, et terminées à leur point de concours. L'équation (1) résulte d'ailleurs de la formule connue $R = \frac{a.b.c}{4S}$. Dès lors, si l'on prend, sur la courbe considérée, les extrémités d'un *diamètre* AA', ou deux points *fixes* A et A' tels, que les tangentes en ces points soient parallèles; et si, ayant mené la tangente $tmt'$ en un point quelconque $m$ de la courbe,

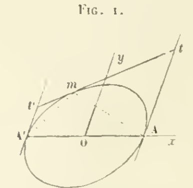
on applique la relation (1) aux deux systèmes de points $m$ et A, $m$ et A'; l'on aura

$$(2)\qquad \frac{\rho}{R} = \left(\frac{mt}{At}\right)^3,$$

$$(3)\qquad \frac{\rho}{R'} = \left(\frac{mt'}{At'}\right)^3;$$

R et R' désignant les rayons de courbure pour les points A et A'. D'ail-

Fig. 1.




leurs ces rayons R et R' sont égaux; cela résulte encore, implicitement, de la formule (1): et l'on a, par suite,

$$(4)\qquad \frac{mt}{mt'} = \frac{At}{At'}.$$

Or cette propriété de la tangente est facile à traduire en analyse : et la démonstration s'achève alors aisément.

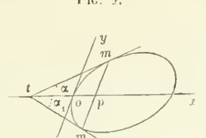
*Remarque.* — La démonstration précédente suppose que l'on puisse trouver un diamètre AA' rencontrant la courbe en deux points : ce qui est toujours possible, en effet, à moins que tous les diamètres ne soient parallèles. Mais, dans ce cas, la droite qui joint le point de concours des tangentes, menées par les extrémités d'une corde, au milieu de cette corde, est parallèle à une direction fixe, la direction des diamètres : Et il en résulte, en rendant fixe l'une des extrémités de la corde, et choisissant des axes convenables, que la *sous-tangente*, en un point quelconque de la courbe considérée, *est double de l'abscisse du point de contact* : ce qui caractérise la *parabole*.

2. Théorème II. — *Si toutes les cordes* concourantes d'*une courbe plane ont leurs* pôles *en ligne droite, cette courbe est du second degré* :

le *pôle* d'une corde n'étant autre chose ici que le point de concours des tangentes menées par ses extrémités.

Supposons seulement que la propriété ait lieu pour tous les systèmes de cordes dont les points de concours sont situés sur une droite déterminée; et faisons la perspective de la figure de manière que cette droite soit *emportée à l'infini* : la perspective nous présentera une courbe telle, que les *pôles* des cordes parallèles à une direction quelconque

Fig. 2.




soient situés en ligne droite. Or il résulte de là que toutes les cordes parallèles $mm_1$ sont divisées dans un rapport constant par la droite $Ox$ qui contient leurs pôles : $\frac{mp}{m_1 p} = \frac{k}{1}$. On a, en effet,

$$\frac{dy}{dx} = \frac{y}{pt}, \quad \frac{dy_1}{dx} = \frac{y_1}{pt}; \quad \frac{dy}{y} = \frac{dy_1}{y_1}, \quad \frac{y}{y_1} = k.$$

En outre, ce rapport constant $k$ est égal à l'unité. Car on trouve, pour le rapport des rayons de courbure aux extrémités de la corde $mm_1$,

$$\frac{\rho}{\rho_1} = \frac{1}{k}\left(\frac{mt}{m_1 t}\right)^3,$$

ou encore

$$\frac{\rho}{\rho_1} = k^2\left(\frac{\sin\alpha_1}{\sin\alpha}\right)^3.$$

D'ailleurs, quand les deux points $m$, $m_1$ tendent simultanément vers le point O, le rapport précédent tend vers $k^2$; il doit, en réalité, tendre vers l'unité; donc $k = 1$. La droite $Ox$, qui contient les pôles des cordes parallèles $mm'$, est un diamètre de ces cordes; tout système de cordes parallèles admet un diamètre rectiligne, et nous rentrons dans le théorème précédent.

3. Théorème III. — *Si une courbe à centre admet une infinité de systèmes de rayons vecteurs conjugués,* ou tels, que la tangente, menée par l'extrémité de l'un quelconque des deux rayons, soit parallèle à l'autre : *L'aire du parallélogramme construit sur deux rayons vecteurs conjugués est constante; et la courbe est l'enveloppe d'une série d'ellipses de même centre et de même surface.*

Considérons, en effet, le parallélogramme inscrit dans la courbe, et ayant pour sommets les quatre extrémités de deux rayons vecteurs conjugués quelconques $aoa'$, $bob'$. Ce parallélogramme est *maximum d'aire,* parmi tous les quadrilatères que l'on peut inscrire dans la courbe, parce que la tangente en chacun des sommets est parallèle à la diagonale qui réunit les sommets adjacents. Il en est de même pour chacun des parallélogrammes que l'on peut construire de la même manière; et, par suite, tous *ces parallélogrammes maximums sont équivalents.* D'ailleurs, si l'on construit l'ellipse auxiliaire, définie par les deux *diamètres conjugués* $aoa'$, $bob'$; la courbe proposée sera tangente en $a$, $b$, $a'$ et $b'$ à cette ellipse, et sera la commune enveloppe de toutes les ellipses analogues, lesquelles ont même centre et même surface.

4. Théorème IV. — *Si le sommet d'un angle droit, circonscrit à une courbe plane, décrit une ligne droite; et si, en même temps, la corde qui réunit les points de contact des côtés de cet angle passe par un point fixe : cette courbe est une parabole.*

Quoique la démonstration de ce théorème paraisse d'abord dépendre du calcul aux différences mêlées, l'analyse exacte et géométrique de *toutes les données* de la courbe permet d'obtenir son équation différentielle sous la forme ordinaire. On trouve ainsi l'équation

$$\frac{p^2}{r} = \text{constante},$$

$r$ désignant le rayon vecteur et $p$ la distance de l'*origine* à la tangente.

II.

5. Théorème V. — *Toute surface qui admet deux modes distincts*

*de génération par un cercle dont le plan demeure parallèle à un plan fixe, est une surface du second degré.*

Prenons, en effet, pour axe des $z$ la corde commune à deux des cercles de la surface, situés dans les plans obliques $zy$, $zx$, et représentés par les équations

$$(1) \qquad \begin{cases} x = 0, \\ z^2 + y^2 + By + C = 0; \end{cases}$$

$$(2) \qquad \begin{cases} y = 0, \\ z^2 + x^2 + Ax + C = 0: \end{cases}$$

l'*origine* étant placée au milieu de la corde commune.

Si, prenant alternativement le premier ou le second de ces cercles pour cercle *directeur*, on cherche l'équation de la surface engendrée par un cercle variable, parallèle au plan du second cercle ou du premier, et rencontrant constamment en deux points réels le cercle directeur, on trouvera cette double équation de la surface cherchée

$$(\mathrm{I}) \qquad z^2 + y^2 + x^2 + By - 2x.\psi(y) + C = 0,$$

$$(\mathrm{II}) \qquad z^2 + y^2 + x^2 + Ax - 2y.\varphi(x) + C = 0,$$

$\psi(y)$ et $\varphi(x)$ étant des fonctions *arbitraires* de la seule variable qu'elles renferment.

La surface cherchée, qui admet les deux modes de génération, est donc représentée, indifféremment, par l'une ou l'autre de ces équations; et celles-ci, par conséquent, doivent devenir identiques, après la multiplication de l'une d'elles par un coefficient constant. Ce coefficient d'ailleurs est égal à l'unité, puisque les deux équations ne contiennent qu'un seul terme en $z$, le terme $z^2$, affecté du même coefficient dans l'une et dans l'autre. Les deux équations sont donc actuellement identiques; et l'on voit, en négligeant les parties communes, que les fonctions $\varphi$ et $\psi$, primitivement arbitraires, doivent être telles, que l'on ait, quels que soient $x$ et $y$, l'*identité*

$$Ax - 2y.\varphi(x) = By - 2x.\psi(y),$$

ou celle-ci,

$$[A + 2\psi(y)]x = [B + 2\varphi(x)]y,$$

ou cette dernière enfin,

$$\frac{A + 2\psi(y)}{y} = \frac{B + 2\varphi(x)}{x}$$

qui exige, évidemment, que chacun des deux membres se réduise à une constante C'. On a donc

$$\frac{A + 2\psi(y)}{y} = C',$$

$$2\psi(y) = C'y - A;$$

et la substitution de cette valeur dans (I) donne enfin, pour la surface cherchée, l'équation du *second degré*

$$(\text{I}) \qquad z^2 + y^2 + x^2 - C'xy + By + Ax + C = 0.$$

*Autre démonstration.* — Considérons une surface S qui admette les deux modes de génération dont il s'agit : soient C, Γ deux cercles *déterminés* de la surface, ayant deux points réels communs, et faisant partie des deux séries de sections circulaires ; et soit, en dehors de ces cercles, $m$ un point *déterminé* de la surface. Considérons, en même temps, la surface du second degré Σ assujettie à passer par le cercle C, par le cercle Γ et par le point $m$. Cette surface est déterminée par ces conditions qui équivalent à la donnée de *neuf* points, à savoir : le point $m$ donné explicitement ; les *cinq* points auxquels équivaut la donnée première du cercle C, et les *trois* derniers points auxquels équivaut la donnée seconde du cercle Γ qui a déjà deux points réels communs avec le précédent ; et je dis que la surface primitive S se confond avec la nouvelle surface Σ.

En effet, si l'on mène d'abord par le point $m$ commun aux deux surfaces un plan parallèle au plan du cercle C, commun à l'une et à l'autre ; ce plan devra couper les deux surfaces suivant des cercles, et ces cercles ayant trois points communs (le point $m$, et les deux points réels du cercle Γ situés dans le plan sécant), se confondent en un seul

Soit C′ ce cercle commun. Si l'on coupe ensuite les deux surfaces par un plan quelconque, parallèle au plan du cercle Γ, les sections obtenues seront encore des cercles, dans les deux surfaces; et ces cercles ayant quatre points réels communs (les quatre points déterminés par le plan sécant sur les cercles C et C′ communs aux deux surfaces) se confondent encore en un seul. Les deux surfaces S et Σ se confondent donc elles-mêmes, et la surface S est du second degré.

*Remarque.* — Ce théorème ne paraîtra pas sans intérêt si l'on remarque qu'il existe des surfaces algébriques d'un degré supérieur au second, admettant *deux*, *trois* ou même *quatre* séries de sections circulaires, non situées dans des plans parallèles. Le parallélisme des plans de ces sections caractérisant dès lors, d'une manière exclusive, les surfaces du second degré.

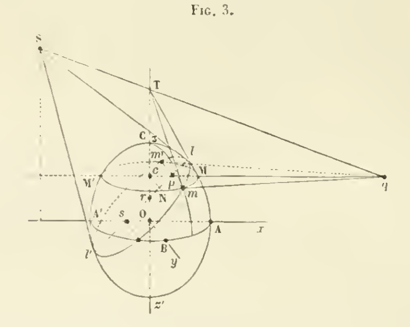
6. Théorème VI. — *Une série de lignes de niveau d'une surface étant composée d'ellipses semblables, semblablement placées et ayant leurs centres en ligne droite: si la courbe de contact d'un cône circonscrit à la surface est plane, cette surface est du second degré*; le cas excepté où le sommet du cône circonscrit donné appartiendrait à la droite des centres Oz.

Nous remarquerons d'abord, en appelant *méridiennes* les sections déterminées dans la surface par les plans menés suivant l'*axe des centres* Oz, que toutes les tangentes, menées aux sections méridiennes par les différents points d'une même ellipse de niveau, vont couper l'axe en un même point T; chaque ellipse de niveau étant dès lors la base d'un cône circonscrit à la surface, et dont le sommet appartient à l'axe : cela se déduit très-simplement de la similitude de forme et de position des ellipses de niveau.

En outre, si nous considérons la corde commune à la courbe de contact *lml′* du cône donné et à l'une quelconque des ellipses de niveau M*m*M′, nous reconnaîtrons que *cette corde mm′*, dont la direction est fixe, *est conjuguée au diamètre c*M, trace de l'ellipse de niveau sur le plan de la *section principale* : en appelant ainsi la section *z*OA menée par l'axe Oz et le sommet S du cône circonscrit. En effet, les points *m* et *m′*, extrémités de cette corde, appartenant à la courbe de contact *lml′* du cône circonscrit donné, les plans tangents à la surface

en ces points passent l'un et l'autre par le sommet S de ce cône; et, ces points appartenant à l'ellipse de niveau $MmM'$, ces mêmes plans

Fig. 3.



tangents passent aussi par le point T, de l'axe $Oz$, qui est le sommet du cône circonscrit à la surface suivant l'ellipse $MmM'$. La droite ST représente donc l'intersection des plans tangents considérés, et sa trace $q$, sur le plan de l'ellipse de niveau, n'est autre chose que le point de concours des tangentes de l'ellipse aux points $m$ et $m'$. Mais la droite ST est dans le plan de la section principale; sa trace $q$ est donc sur le *diamètre principal* $c$M de l'ellipse. Les tangentes aux extrémités de la corde $mm'$ vont concourir sur ce diamètre $c$M, qui est, par suite, conjugué à cette corde.

Nous prendrons dès lors pour axes de coordonnées $Ox$, $Oy$, $Oz$, le *diamètre principal* OA de l'une quelconque des ellipses de niveau, son conjugué OB qui représente la direction générale des cordes $mm'$, et l'axe $Oz$ déja défini; le plan de la courbe de contact, et le sommet S du cône donné étant représentés par les équations

(P) $$x = k(z - c),$$

(S) $$\begin{cases} x = \alpha, \\ y = 0, \\ z = \gamma: \end{cases}$$

et comme il suffira, pour démontrer le théorème, d'établir que l'une

quelconque des sections par l'axe est une courbe du second degré, nous chercherons seulement l'équation différentielle de la *section principale* $z$MA, que l'on peut obtenir d'abord par la géométrie.

En effet, nous avons reconnu précédemment que *les trois points* S, T *et* $q$ *sont en ligne droite*. Or le point S est un point fixe dont les coordonnées, prises dans le plan $zx$, sont

$$(1)\qquad \begin{cases} x_1 = \alpha, \\ z_1 = \gamma. \end{cases}$$

Le point T est la trace, sur l'axe O$z$, de la tangente en $m$ de la section $zm$, ou de la tangente au point correspondant M de la section principale $z$ MA; et les coordonnées du point M, prises dans le plan $zx$, étant $x$, $z$, l'on a $Z - z = \frac{dz}{dx}(X - x)$ pour la tangente en M; d'où

$$(2)\qquad \begin{cases} x_2 = 0, \\ z_2 = z - \dfrac{xdz}{dx}, \end{cases}$$

pour les coordonnées du point T. Enfin le point $q$ est la trace, sur le diamètre principal $c$M de l'ellipse M$m$N, de la tangente menée à cette ellipse par l'une des extrémités de la corde $mm'$ conjuguée à ce diamètre. D'ailleurs, le pied de la corde $mm'$ sur son diamètre étant le point $p$, et $c$ étant le centre de l'ellipse, on a la relation connue

$$\overline{cq}.\overline{cp} = \overline{c\text{M}}^2 = x^2;$$

et comme le point $p$ appartient à une droite fixe, $ll'$ ou $rs$, trace du plan de contact du cône donné S sur le plan $zx$, l'on a

$$\overline{cp} = k.\overline{cr},$$

ou

$$\overline{cp} = k(z - c),$$

$k$ et $c$ désignant des constantes. Par suite, les coordonnées du point $q$ sont les suivantes,

$$(3)\qquad \begin{cases} x_3 = \dfrac{x^2}{k(z-c)}, \\ z_3 = z; \end{cases}$$

et en exprimant que les points (1), (2), (3) sont en ligne droite, l'on trouve, après quelques simplifications,

$$(4)\qquad \frac{x\,dx}{dz} = \frac{x^2 - k\alpha(z - c)}{z - \gamma}$$

pour équation différentielle de la section principale $z$MA. De là, en posant

$$(\mathrm{A})\qquad \begin{cases} x^2 = \mathrm{Y}, \\ z \;= \mathrm{X}, \end{cases}$$

l'on déduit

$$(5)\qquad \frac{d\mathrm{Y}}{d\mathrm{X}} - \frac{2}{\mathrm{X} - \gamma}\mathrm{Y} = -\frac{2k\alpha(\mathrm{X} - c)}{\mathrm{X} - \gamma};$$

équation *linéaire*, de la forme $\frac{dy}{dx} + \mathrm{P}y = \mathrm{Q}$, et dont l'intégrale

$$(6)\qquad \mathrm{Y} = \mathrm{C}(\mathrm{X} - \gamma)^2 + 2k\alpha(\mathrm{X} - \gamma) + k\alpha(\gamma - c)$$

devient, par le retour à la notation primitive (A),

$$(7)\qquad x^2 = \mathrm{C}(z - \gamma)^2 + 2k\alpha(z - \gamma) + k\alpha(\gamma - c).$$

La section principale est donc une courbe du second degré, une ellipse par exemple, ayant son centre sur l'axe O$z$, et rapportée, dans O$x$ et O$z$, à deux directions conjuguées : de telle sorte que, si le point O est supposé le centre de cette ellipse, *la surface proposée est identique à l'ellipsoïde* qui serait *défini* par les trois diamètres conjugués OA, OB et O$z$ ou OC.

On peut parvenir autrement, et par le calcul seul, à l'équation de la section méridienne.

En effet, de la nature des sections déterminées dans la surface par des plans parallèles au plan des $xy$, l'on déduit cette première équation de la surface

$$(1')\qquad m^2 x^2 + y^2 - m^2 f(z) = 0:$$

$m$ étant un coefficient constant, qui mesure le rapport des diamètres conjugués OB et OA des ellipses de niveau, et $f(z)$ désignant une fonc-

tion, encore indéterminée, de la seule variable $z$. Si l'on forme ensuite l'équation du plan tangent en un point $(x, y, z)$ de la surface, et si l'on exprime que ce plan tangent passe par le point donné $S(x = \alpha, y = 0, z = \gamma)$, on trouve

$$(\alpha - x) m^2 x - y^2 - \frac{m^2}{2}(\gamma - z) . f'(z) = 0,$$

qui, combinée avec l'équation (1'), représente la courbe de contact du cône, de sommet S, circonscrit à la surface. Mais, dans cette combinaison des deux équations, on peut simplifier la seconde au moyen de la première ; et il vient ainsi,

$$\alpha . m^2 x - \frac{m^2}{2}(\gamma - z) . f'(z) - m^2 . f(z) = 0,$$

ou, en divisant par $m^2$,

$$(2') \qquad 2\alpha x - (\gamma - z) . f'(z) - 2f(z) = 0.$$

D'ailleurs la courbe de contact du cône considéré est plane, par hypothèse ; et son plan, comme on l'a démontré, est parallèle à $Oy$ : on a donc aussi

$$(3') \qquad x = k(z - c),$$

$k$, $c$ désignant de nouvelles constantes ; et si l'on porte cette valeur de $x$ en $z$ dans (2'), il vient l'identité suivante, propre à déterminer la fonction $f(z)$,

$$(4') \qquad 2k\alpha(z - c) - (\gamma - z) . f'(z) - 2f(z) = 0.$$

De là, en posant

$$(A') \qquad \begin{cases} Y = f(z), \\ X = z, \end{cases}$$

l'on déduit

$$(5') \qquad \frac{dY}{dX} - \frac{2}{X - \gamma} Y = - 2k\alpha \cdot \frac{X - c}{X - \gamma} :$$

Équation identique à l'équation (5), et conduisant aux mêmes conséquences.

*Remarque.* — Le théorème que nous venons de démontrer est une généralisation du suivant, dû à M. de la Gournerie : « Une surface de révolution, qui admet une ligne d'ombre plane, est du second degré. » Il convient toutefois, afin de bien apprécier l'utilité de notre généralisation, de remarquer que le nombre des conditions sous lesquelles on affirme, dans l'énoncé précédent, que la surface est du second degré, paraît plus restreint qu'il ne l'est en réalité ; puisque l'existence d'une première ligne d'ombre plane, dans une surface de révolution, entraîne l'existence d'une infinité d'autres lignes analogues, obtenues en faisant tourner la première d'un angle quelconque autour de l'axe.

7. Théorème VII. — *Si les cônes et les cylindres, circonscrits à une surface, ont leurs courbes de contact planes, cette surface est du second degré.*

Que l'on imagine une série de *lignes de niveau* de la surface ; les cylindres circonscrits à la surface parallèlement aux diverses directions tracées dans le plan de l'une de ces lignes, et la série correspondante des courbes de contact de ces cylindres : il résulte, de l'hypothèse, que chacune de ces courbes est plane, et que chaque ligne de niveau est la base d'un cône circonscrit à la surface. On peut donc considérer, *en chaque point de la surface*, deux systèmes de *tangentes conjuguées*. La génératrice du cône circonscrit, et la tangente à la ligne de niveau qui sert de base à ce cône (premier système) ; la génératrice du cylindre circonscrit, et la tangente à la courbe de contact de ce cylindre (second système). Mais la génératrice du cylindre coïncide avec la tangente de la ligne de niveau, par une suite à peu près immédiate de la définition du cylindre ; nos deux systèmes de tangentes conjuguées ont donc une tangente commune : les autres tangentes coïncident, et la génératrice du cône coïncide avec la tangente à la courbe de contact du cylindre. Le sommet du cône relatif à l'une quelconque des lignes de niveau est donc situé dans le plan de contact de l'un quelconque des cylindres déjà définis. Donc, *les plans de contact de tous ces cylindres se coupent suivant une même droite*, et *cette droite contient les sommets des cônes relatifs à toutes les lignes de niveau.*

Que l'on compare maintenant deux lignes de niveau quelconques; et que l'on prenne, pour origine des rayons vecteurs de chacune de ces lignes, le point où son plan est rencontré par la droite précédente : on reconnaîtra sans peine que les tangentes, menées à ces lignes par les extrémités de deux rayons vecteurs parallèles, sont elles-mêmes parallèles; d'où la conséquence que *toutes les lignes de niveau sont des courbes semblables, semblablement placées, et ayant leurs centres de similitude en ligne droite*. Les sections, faites dans la surface proposée par des plans parallèles à une direction quelconque, sont donc des courbes semblables; l'on rentre dans un théorème dû à M. Bertrand (*Journal de Mathématiques*, p. 77, t. XIII, 1848), et la surface est du second degré.

*Remarque I.* — On peut achever la démonstration autrement, et sans recourir au théorème auquel il a été fait allusion. Ce changement n'aurait en lui-même aucun avantage, s'il ne devait permettre de diminuer le nombre des conditions sous lesquelles on peut affirmer que la surface est du second degré; et c'est ce qui arrive ici. Il résulte, en effet, de la théorie des tangentes conjuguées et des considérations dont nous ferons usage dans les théorèmes suivants, que les lignes de niveau dont il a été question sont des *ellipses*, ayant leurs centres sur la droite qui contient les sommets des cônes relatifs à ces lignes, *homothétiques entre elles* et à l'ellipse qui sert d'indicatrice à la surface aux points où celle-ci est rencontrée par la droite des sommets. L'on rentre donc dans le cas du théorème VI, et l'on a ce nouvel énoncé :

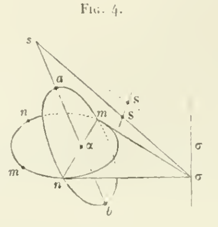
Théorème VIII. — *Si les cylindres circonscrits à une surface, parallèlement au plan tangent en l'un de ses points, ont leurs courbes de contact planes; et si les diverses sections de la surface, parallèles au même plan tangent, sont les bases d'autant de cônes circonscrits : cette surface sera du second degré, dès qu'elle admettra un nouveau cône, ou un nouveau cylindre, à courbe de contact plane.* Il convient d'ajouter toutefois que le point de la surface, qui joue un rôle spécial dans l'énoncé, doit n'être pas un *point singulier*, afin que le théorème d'Euler puisse s'appliquer à ce point.

*Remarque II.* — Le théorème VII est susceptible d'une autre dé-

monstration, assez curieuse en ce que la théorie des surfaces n'y joue aucun rôle.

Soit un cône *déterminé*, de sommet $s$, circonscrit à la surface suivant

Fig. 4.




la courbe plane *mnmn*. Que l'on mène, par le sommet $s$, une droite quelconque *sab* rencontrant la surface aux points $a$ et $b$, et que l'on imagine toutes les sections faites dans la surface par les plans menés suivant *sab*. Ces sections *manb* sont les bases d'autant de cônes circonscrits dont *les sommets* S *sont distribués sur une même droite* SS, intersection des plans tangents menés à la surface par les points $a$ et $b$. Si l'on considère le point de concours des tangentes menées à la première courbe *mn*, par ses points de rencontre $m$ et $n$ avec l'une quelconque des nouvelles courbes *manb*, on reconnaît que ce point de concours est situé sur la droite $s$S, commune intersection des plans tangents à la surface en $m$ et $n$. Or, comme toutes les droites analogues $s$S sont situées dans un même plan, on voit, en appelant $\alpha$ et $\overline{\sigma\sigma}$ les traces de la droite *sab* et du plan $s$SS sur le plan de la courbe primitive *mnmn*, que les points de concours des tangentes à cette courbe, menées par les extrémités de toutes les cordes $m\alpha n$ qui se croisent au point $\alpha$, sont distribués sur une même droite $\sigma\sigma$; et cette propriété subsiste, quelle que soit la position de la droite S*ab* autour du point $s$, ou quel que soit le point $\alpha$, trace de cette droite sur le plan de la courbe *mn*. Cette courbe *mnmn* est donc telle, que « toutes les cordes concourantes de cette courbe ont leurs *pôles* en ligne droite »; le théorème II est applicable, la courbe *mn* et la surface proposée sont du second degré.

8. Théorème IX. — *Si les cônes, circonscrits à une surface, se cou-*

*peut, deux à deux, suivant des courbes planes, cette surface est du second degré.*

Soient, en effet, un cône *fixe*, de sommet $s$, et un cône variable dont le sommet $s'$ se rapproche indéfiniment du premier. La ligne formée par l'intersection de ces cônes sera une certaine courbe *plane*, variant de forme et de position en même temps que le second cône, et ayant pour limite une courbe plane. D'ailleurs, cette courbe limite n'est autre que la courbe de contact du cône fixe et de la surface proposée. Tous les cônes circonscrits à la surface ont donc leur courbe de contact plane; l'on rentre dans le théorème VII, et la surface est du second degré.

**9.** Théorème X. — *Si les cônes circonscrits à une surface sont du second degré, cette surface elle-même est du second degré.*

Que l'on considère, en effet, deux *quelconques* des cônes du second degré circonscrits à la surface. Ces cônes auront *deux plans tangents communs*, à savoir les deux plans tangents que l'on peut mener à la surface proposée par la droite qui réunit leurs sommets. L'intersection de ces deux cônes forme donc, suivant une proposition bien connue, un système de deux courbes planes; et l'on rentre, si l'on veut, dans le théorème précédent.

**10.** Théorème XI. — *Si toutes les sections planes, menées suivant un axe* Oz, *sont les courbes de contact d'autant de cylindres circonscrits à la surface; l'équateur* AB *de la surface,* c'est-à-dire la courbe de contact d'un cylindre circonscrit parallèle à l'axe, *est une ellipse plane; les sections faites dans la surface, parallèlement aux plans tangents menés par les extrémités de l'axe, sont des ellipses homothétiques à la précédente; et les centres de toutes ces ellipses sont situés sur l'axe :* le mot *axe* n'entraînant ici aucune idée d'orthogonalité ou de symétrie, et servant seulement à désigner la droite qui réunit, dans une surface quelconque, les points de contact de deux plans tangents parallèles, ou deux *pôles* quelconques de la surface.

Considérons, en effet, un point quelconque A de l'équateur AB; et la section par l'axe, ou section méridienne, $z$A$z'$, qui passe par ce point et s'y trouve tangente à la génératrice du cylindre circonscrit à la sur-

face suivant l'équateur, ainsi que cela résulte de la définition de celui-ci. Nous aurons, au point considéré, deux systèmes de tangentes conjuguées. La génératrice du cylindre circonscrit suivant l'équateur, et la tangente de l'équateur (premier système); la génératrice du cylindre circonscrit suivant la ligne méridienne, et la tangente de cette ligne (second système). D'ailleurs ces deux systèmes de tangentes conjuguées ayant une droite commune (la génératrice du cylindre relatif à l'équateur, génératrice qui coïncide avec la tangente de la méridienne), les autres droites coïncident : et la tangente en un point quelconque de l'équateur coïncide avec la génératrice du cylindre relatif à la méridienne. Mais cette génératrice est parallèle au plan tangent au pôle $z$; donc toutes les tangentes de l'équateur sont parallèles à ce plan. *L'équateur est une ligne plane, et son plan est parallèle au plan tangent au pôle.*

Soit maintenant O la trace de l'axe $zOz'$ sur le plan de l'équateur. Prenons ce point O pour origine des rayons vecteurs OA de l'équateur; et, supposant tracée dans le plan tangent au pôle $z$, autour de ce point comme centre, l'ellipse qui sert d'indicatrice à la surface en ce point : imaginons le demi-diamètre de cette ellipse qui est parallèle au rayon vecteur OA de l'équateur, ainsi que la tangente à l'extrémité de ce diamètre. Puisque celui-ci est tangent à la section méridienne $z$A, cette tangente de l'ellipse est parallèle aux génératrices du cylindre relatif à la méridienne, comme l'est déjà la tangente au point correspondant de l'équateur. Les tangentes de l'indicatrice et de l'équateur, en des points de ces lignes qui correspondent à des rayons vecteurs parallèles, sont donc parallèles : ces deux lignes sont *homothétiques*, et l'équateur est une *ellipse* ayant pour centre le point O, trace de l'axe O$z$ sur son plan, comme l'indicatrice est une ellipse ayant pour centre le pôle $z$.

On trouverait, d'une manière toute semblable, la nature des sections faites dans la surface parallèlement au plan tangent au pôle, que l'on suppose n'être pas un point singulier.

11. Théorème XII. — *Si les cylindres, circonscrits à une surface, ont leurs courbes de contact planes; cette surface est du second degré.*

Nous établirons d'abord que : *tous les plans des courbes de contact qui se croisent en un même point z de la surface, se coupent suivant une même droite zz'*.

Considérons, à cet effet, la droite $zz'$, intersection des plans de deux de ces courbes $zAz'$, $zBz'$; et la courbe de contact AB du cylindre circonscrit à la surface parallèlement à cette droite $zz'$. En vertu de l'hypothèse, cette troisième courbe AB est plane; et l'on verrait, comme dans le théorème précédent, que les tangentes de cette courbe, aux points A et B où elle est rencontrée par les deux premières $zA$ et $zB$, coïncident avec les génératrices des cylindres relatifs à ces lignes, en se trouvant, par suite, parallèles au plan tangent de la surface en $z$. Le plan de la courbe AB elle-même est donc parallèle au plan tangent en $z$.

Dès lors, si les plans de toutes les courbes de contact $zA$, $zB$,..., qui se croisent en $z$, ne se coupaient pas suivant une droite unique $zz'$, les intersections de ces plans, pris deux à deux, donneraient naissance à une infinité de droites analogues à la droite $zz'$; et la surface admettrait une infinité de sections planes parallèles au plan tangent en $z$, et servant de bases à une infinité de cylindres circonscrits parallèles à ces différentes droites; ce qui est absurde.

Les plans des courbes de contact, qui se croisent en un point quelconque $z$ de la surface, se coupent donc suivant une même droite $zz'$; nous rentrons dans le cas du théorème XI, et toutes les sections de la surface, parallèles au plan tangent en $z$, sont des ellipses homothétiques ayant leurs centres sur la droite $zz'$. Le théorème V est donc applicable à son tour, et la surface est du second degré.

*Remarque I.* — Pour achever la démonstration sans recourir au théorème V, il suffit d'appliquer les propriétés trouvées pour un point quelconque $z$ de la surface, à l'un des points A de l'*ellipse* de contact AB du cylindre circonscrit à la surface parallèlement à la droite $zOz'$. Car, ayant reconnu que l'*axe commun* aux plans des courbes de contact qui se croisent au point A, est précisément le diamètre OA; nous verrions que la courbe de contact du cylindre circonscrit, parallèle à l'axe OA, est une nouvelle ellipse plane, passant par les points $z$, $z'$ et par les extrémités du diamètre BOB', conjugué du diamètre AOA' : la surface étant dès lors identique à l'ellipsoïde qui serait défini par les trois diamètres conjugués AOA', BOB', $zOz'$.

*Remarque II.* — Enfin la combinaison des théorèmes V et XI conduit à ce nouvel énoncé :

Théorème XIII. — *Si les cylindres circonscrits à une surface, parallèlement au plan tangent en un point non singulier de la surface, ont leurs courbes de contact planes; et si les plans de ces courbes se coupent suivant une même droite : cette surface sera du second degré, dès qu'elle admettra* un nouveau *cylindre, ou un cône, à courbe de contact plane.*

12. Théorème XIV. — *Si,* dans la série infinie des courbes de contact des cylindres circonscrit à une surface, *les plans osculateurs de toutes celles de ces courbes qui se croisent en chaque point* O *de la surface, se coupent suivant une même droite : cette surface est du second degré.*

Nous allons, du moins, établir la proposition pour le cas, assez étendu, ou l'*indicatrice de la surface*, en tous les points de celle-ci, *est une hyperbole;* et cela suffira pour mettre hors de doute la proposition générale.

Considérons donc, en un point quelconque O de la surface, les deux *lignes asymptotiques* OA, OB qui se croisent en ce point en ayant pour tangentes les asymptotes de l'hyperbole qui sert d'indicatrice à la surface au point O : et, parmi les cylindres dont les courbes de contact se croisent en ce point, considérons spécialement ceux dont les génératrices sont parallèles aux asymptotes de l'indicatrice; et soient O$a$, O$b$ leurs courbes de contact.

La tangente en O de la courbe O$a$, et la génératrice du cylindre correspondant, sont deux tangentes conjuguées; mais la génératrice du cylindre coïncide avec l'une des asymptotes de l'indicatrice, et cette asymptote représente un système de deux tangentes conjuguées, confondues en une seule. Donc la courbe de contact O$a$ du cylindre considéré est tangente en O à la génératrice du cylindre; et dès lors, par un théorème connu, *le plan osculateur en* O *de la courbe* O$a$ *coïncide* avec le plan tangent du cylindre, ou *avec le plan tangent de la surface primitive au même point.* Mais, d'après l'hypothèse, les plans osculateurs de toutes les courbes de contact qui se croisent en O, se coupent

suivant une même droite; on vient de voir que l'un de ces plans coïncide avec le plan tangent de la surface pour le point O; donc la droite, intersection commune de tous les plans osculateurs, est située dans *le plan tangent qui représente*, dès lors, *le plan osculateur commun à toutes les courbes de contact* O$a$, O$b$, O$c$. Or, il résulterait de là, que la génératrice en O de chacun de ces cylindres se confondrait avec la tangente au même point de la courbe de contact correspondante. La surface admettrait, *en chacun de ses points* O, une infinité de systèmes de tangentes conjuguées confondues en une seule; et, l'indicatrice, une infinité d'asymptotes : ce qui est absurde.

L'hypothèse contenue dans l'énoncé ne peut donc se réaliser, à moins que les plans osculateurs des deux courbes de contact O$a$, O$b$, ne deviennent *indéterminés*. D'ailleurs ces courbes sont respectivement tangentes aux lignes asymptotiques OA, OB; les plans osculateurs de ces quatre lignes coïncident deux à deux, et ces plans osculateurs ne deviennent indéterminés que dans le cas où *les lignes asymptotiques* OA *et* OB *deviennent des lignes droites*. Il passe donc, en chaque point de la surface proposée, deux lignes droites situées sur la surface : celle-ci admet deux systèmes de génératrices rectilignes, et n'est autre qu'une surface gauche du second degré.

---

# THÉORÈMES

CONCERNANT

## LE DOUBLE D'UN NOMBRE PREMIER DE LA FORME $16k+7$;

PAR M. J. LIOUVILLE.

Le double ($2m$) de tout nombre premier $m$ de la forme $16k+7$ jouit des deux propriétés ci-après :

1° On peut poser au moins une fois (et toujours un nombre impair de fois) l'équation

$$2m = (8x+1)^2 + q^{4l+1}y^2,$$

$x$ étant un entier indifféremment positif, nul ou négatif, d'ailleurs pair ou impair, tandis que $y$ est impair et positif : quant à $q$, c'est un nombre premier $(8g+5)$ qui ne divise pas $y$ : on admet pour $l$ la valeur zéro.

En d'autres termes, si du double d'un nombre premier donné $m$ de la forme $16k+7$, on retranche, tant que faire se peut, les carrés

$$1^2,\ 7^2,\ 9^2,\ 15^2,\ 17^2,\ldots,$$

fournis par la formule

$$(8x+1)^2,$$

en y prenant $x$ positif, nul ou négatif, il y aura un nombre impair de restes exprimables par le produit

$$q^{4l+1}y^2,$$

$q$ étant un nombre premier non diviseur de $y$ et naturellement de la forme $8g+5$.

2° On peut de même poser au moins une fois (et toujours un nombre impair de fois) l'équation

$$2m = (8x + 3)^2 + q^{4l+1} y^2,$$

$x$ étant un entier indifféremment positif, nul ou négatif, tandis que $y$ est impair et positif, $q$ continuant à désigner un nombre premier $8g + 5$ non diviseur de $y$, et la valeur $l = 0$ restant admise.

En d'autres termes, si du double d'un nombre premier donné $m$ de la forme $16k + 7$, on retranche, tant que faire se peut, les carrés

$$3^2,\ 5^2,\ 11^2,\ 13^2,\ 19^2, \ldots,$$

fournis par la formule

$$(8x + 3)^2,$$

en y prenant $x$ indifféremment positif, nul ou négatif, il y aura un nombre impair de restes exprimables par le produit

$$q^{4l+1} y^2,$$

$q$ étant un nombre premier non diviseur de $y$ et naturellement de la forme $8g + 5$.

Nous donnerons plus tard la démonstration (fort simple) de ces deux théorèmes. Bornons-nous aujourd'hui à les vérifier numériquement sur quelques exemples.

Soit d'abord

$$m = 7.$$

Nous aurons d'une part

$$2.7 = 1^2 + 13.1^2,$$

conformément au premier théorème, et d'autre part

$$2.7 = 3^2 + 5.1^2,$$

conformément au second théorème.

Soit ensuite

$$m = 23:$$

nous aurons semblablement deux équations canoniques

$$2.23 = 1^2 + 5.3^2$$

et

$$2.23 = 3^2 + 37.1^2.$$

De même pour

$$m = 71,$$

on a

$$2.71 = 9^2 + 61.1^2$$

et

$$2.71 = 5^2 + 13.3^2.$$

Il serait inutile d'ajouter d'autres exemples. Mais en terminant nous remarquerons, comme conséquence immédiate de nos deux théorèmes, que pour chaque nombre premier $m$ de la forme $16k + 7$, le nombre des solutions de l'équation

$$2m = x^2 + q^{4l+1} y^2$$

est pair, mais au moins égal à 2, lorsqu'on admet pour $x$ comme pour $y$ des valeurs impaires quelconques, $q$ continuant à être un nombre premier $(8g + 5)$ qui ne divise pas $y$.

# THÉORÈME

## CONCERNANT LES NOMBRES PREMIERS DE LA FORME $8\mu+1$;

### Par M. J. LIOUVILLE.

Soit $m$ un nombre premier donné, de la forme $8\mu+1$ : on pose de toutes les manières possibles l'équation

$$m = 4x^2 + q^{4l+1}y^2,$$

en y prenant pour $x$ et $y$ des entiers impairs et pour $q$ les nombres premiers $(8\nu+5)$ non diviseurs de $y$ : on admet pour $l$ la valeur zéro. Il s'agit de savoir si le nombre N des décompositions de $m$ sous la forme indiquée est pair ou impair.

En d'autres termes, on retranche (par la pensée) d'un nombre premier donné $m$, de la forme $8\mu+1$, les carrés des nombres impairement pairs 2, 6, etc., puis considérant le nombre N de ceux des restes qui peuvent se mettre sous la forme

$$q^{4l+1}y^2,$$

où $q$ désigne un nombre premier non diviseur de $y$ et naturellement de la forme $8\nu+5$, on demande une règle facile pour dire à priori si N est pair ou impair.

La réponse que je fais à cette question contentera, je crois, les geometres.

Puisque $m$ est un nombre premier $8\mu+1$, on peut poser d'une seule manière, en nombres entiers,

$$m = a^2 + 8b^2.$$

Or je trouve que l'on a toujours

$$N \equiv b \pmod{2},$$

à savoir N est pair quand $b$ est pair, mais impair quand $b$ est impair.

Ainsi, pour

$$m = 17 = 3^2 + 8.1^2,$$

on a $b = 1$, donc N impair; et c'est ce qui résulte en effet de la décomposition canonique

$$17 = 4.1^2 + 13.1^2.$$

Au contraire, pour

$$m = 41 = 3^2 + 8.2^2,$$

on a $b = 2$, donc N pair; et cela est exact encore, puisque les décompositions canoniques sont ici au nombre de deux :

$$41 = 4.1^2 + 37.1^2,$$
$$41 = 4.3^2 + 5.1^2.$$

# MÉMOIRE

SUR

# LES NOMBRES DE CAUCHY

ET

## LEUR APPLICATION A DIVERS PROBLÈMES DE MÉCANIQUE CÉLESTE;

PAR M. J. BOURGET,
Professeur à la Faculté des Sciences de Clermont-Ferrand.

---

### § I. — *Nombres de Cauchy.*

**1.** Dans un Mémoire sur le développement de la fonction perturbatrice [*], l'illustre géomètre à introduit avec avantage le nombre $N_{-i,j,p}$, défini par l'équation

$$(1)\quad N_{-i,j,p} = \frac{1}{2\pi}\int_0^{2\pi} c^{-iu\sqrt{-1}}\left(c^{u\sqrt{-1}} + c^{-u\sqrt{-1}}\right)^j \left(c^{u\sqrt{-1}} - c^{-u\sqrt{-1}}\right)^p du,$$

$j$ et $p$ étant des nombres nuls, ou entiers et positifs, $i$ étant nul ou entier, ou bien

$$(2)\qquad N_{-i,j,p} = \frac{1}{2\pi}\int_0^{2\pi} x^{-i}\left(x+\frac{1}{x}\right)^j\left(x-\frac{1}{x}\right)^p du,$$

si l'on pose

$$x = c^{u\sqrt{-1}},$$

et si l'on représente par $c$ la base des logarithmes népériens.

En m'occupant des propriétés de ces nombres, j'ai découvert qu'on peut en former un tableau aussi étendu qu'on voudra, analogue au

---

[*] *Comptes rendus de l'Académie*, t. XII, p. 92.

triangle arithmétique de Pascal, et que les nombres figurés n'en sont qu'un cas particulier. J'ai vu de plus qu'un grand nombre de fonctions utiles en astronomie se développent en série avec la plus grande facilité quand on connaît les quantités N. Ajoutons qu'à côté de ces nombres apparaissent naturellement des transcendantes comprenant celle de Bessel, et faciles à calculer à l'aide des nombres N. Je montre qu'à l'aide de ces transcendantes on peut résoudre presque sans calcul le problème de Képler et d'autres analogues. M. Faa de Bruno [*] avait déjà signalé la simplicité avec laquelle la transcendante de Bessel donne l'anomalie excentrique et le rayon vecteur en fonction de l'anomalie moyenne. Les recherches que nous consignons ici complètent et étendent ce travail.

2. *Propriétés des nombres de Cauchy.* — Les propriétés des nombres $N_{-i,j,p}$, dont quelques-unes ont été signalées par Cauchy, se résument dans la série des théorèmes suivants :

Théorème I. — *Le nombre* $N_{-i,j,p}$ *est égal à la partie constante du développement de* $x^{-i}\left(x+\frac{1}{x}\right)^j\left(x-\frac{1}{x}\right)^p$, *suivant les puissances de* $x$.

En effet, tout terme qui dans le développement renferme l'exponentielle $x$, donne zéro par l'intégration.

Théorème II. — *Le nombre* $N_{-i,j,p}$ *est nul toutes les fois que la somme des indices* $-i+j+p$ *est négative ou impaire, et il est égal à l'unité quand cette somme est nulle.*

En effet, le développement du produit

$$x^{-i}\left(x+\frac{1}{x}\right)^j\left(x-\frac{1}{x}\right)^p$$

donne un résultat de la forme

$$x^{j+p-i}+H_1x^{j+p-i-2}+H_2x^{j+p-i-4}+\ldots.$$

---

[*] Thèse présentée à la Faculté de Paris, 1856.

Or il ne peut y avoir un terme indépendant de $x$ qu'autant que

$$j+p-i=2k,$$

$k$ étant un nombre entier positif; et si

$$j+p-i=0,$$

le terme indépendant de $x$ est l'unité.

THÉORÈME III. — *Si $i$ change de signe,* N *garde la même valeur numérique; mais il change de signe si $p$ ou $j-i$ est impair.*

En effet, nous avons identiquement

$$x^{-i}\left(x+\frac{1}{x}\right)^j\left(x-\frac{1}{x}\right)^p=\left(\frac{1}{x}\right)^i\left(\frac{1}{x}+x\right)^j\left(\frac{1}{x}-x\right)^p\left(-1\right)^p;$$

donc, en prenant les parties constantes des deux membres, il vient

$$\mathrm{N}_{-i,j,p}=(-1)^p\,\mathrm{N}_{i,j,p};$$

d'ailleurs

$$(-1)^p=(-1)^{2k-j+i}=(-1)^{j-i},$$

le théorème est donc démontré.

THÉORÈME IV. — *Si l'on connaît tous les nombres* N *relatifs à une certaine valeur de $j$, on peut en déduire ceux qui se rapportent à une valeur de $j$ immédiatement supérieure.*

En effet, on a identiquement

$$x^{-i}\left(x+\frac{1}{x}\right)^j\left(x-\frac{1}{x}\right)^p=x^{-i+1}\left(x+\frac{1}{x}\right)^{j-1}\left(x-\frac{1}{x}\right)^p + x^{-i-1}\left(x+\frac{1}{x}\right)^{j-1}\left(x-\frac{1}{x}\right)^p,$$

ce qui démontre le théorème, car on en déduit

$$\mathrm{N}_{-i,j,p}=\mathrm{N}_{-i+1,j-1,p}+\mathrm{N}_{-i-1,j-1,p}.$$

THÉORÈME V. — *Si l'on connaît tous les nombres* N *relatifs à une*

*certaine valeur de p, on peut en déduire tous ceux qui se rapportent à une valeur de p immédiatement supérieure.*

On démontre, en effet, comme dans le théorème précédent, que

$$N_{-i,j,p} = N_{-i+1,j,p-1} - N_{-i-1,j,p-1}.$$

*Corollaire.* — Les deux derniers théorèmes montrent que le calcul des nombres de Cauchy se ramène au cas où $j$ et $p$ sont nuls.

Théorème VI. — *Il existe une relation entre les nombres N qui correspondent à une même valeur de i et à des valeurs de j et p voisines.*

En effet, on a identiquement

$$x^{-i}\left(x+\frac{1}{x}\right)^j\left(x-\frac{1}{x}\right)^p = \frac{x^{-i}\,D_u\left(x-\frac{1}{x}\right)^{p+1}\cdot\left(x+\frac{1}{x}\right)^{j-1}}{(p+1)\sqrt{-1}}$$

$$= \frac{x^{-i}\,D_u\left(x+\frac{1}{x}\right)^{j+1}\cdot\left(x-\frac{1}{x}\right)^{p-1}}{(j+1)\sqrt{-1}};$$

donc

$$N_{-i,j,p} = \frac{1}{(p+1)\sqrt{-1}}\,\frac{1}{2\pi}\int_0^{2\pi} x^{-i}\left(x+\frac{1}{x}\right)^{j-1} D_u\left(x-\frac{1}{x}\right)^{p+1}.du$$

$$= \frac{1}{(j+1)\sqrt{-1}}\,\frac{1}{2\pi}\int_0^{2\pi} x^{-i}\left(x-\frac{1}{x}\right)^{p-1} D_u\left(x+\frac{1}{x}\right)^{j+1}.du.$$

Intégrons par parties, il vient

$$N_{-i,j,p} = -\frac{1}{(p+1)\sqrt{-1}}\,\frac{1}{2\pi}\int_0^{2\pi} D_u\left[x^{-i}\left(x+\frac{1}{x}\right)^{j-1}\right]\left(x-\frac{1}{x}\right)^{p+1} du$$

$$= -\frac{1}{(j+1)\sqrt{-1}}\,\frac{1}{2\pi}\int_0^{2\pi} D_u\left[x^{-i}\left(x-\frac{1}{x}\right)^{p-1}\right]\left(x+\frac{1}{x}\right)^{j+1} du;$$

en développant, on trouve

$$N_{-i,j,p} = \frac{i}{p+1}\,N_{-i,j-1,p+1} - \frac{j-1}{p+1}\,N_{-i,j-2,p+2}$$

et

$$N_{-i,j,p} = \frac{i}{j+1} N_{-i,j+1,p-1} - \frac{p-1}{j+1} N_{-i,j+2,p-2}.$$

*Corollaires.* — On déduit des relations précédentes

$$N_{-i,1,p} = \frac{i}{p+1} N_{-i,0,p+1}$$

et

$$N_{-i,j,1} = \frac{i}{j+1} N_{-i,j+1,0}.$$

Théorème VII. — *Les deux nombres* $N_{-i,j,0}$ *et* $N_{-i-2,j,0}$, *qui ne diffèrent que par les valeurs de i, sont liés entre eux par l'équation*

$$N_{-i,j,0} = \frac{i+j+2}{j-i} N_{-i-2,j,0}.$$

On peut démontrer ce théorème directement en partant de la définition du nombre N, et procédant par l'intégration par parties; mais on y arrive plus facilement en faisant usage des théorèmes précédents.

Un des corollaires du théorème VI donne

$$(j+1) N_{-i,j,1} = i N_{-i,j+1,0};$$

mais les théorèmes IV et V donnent

$$N_{-i,j,1} = N_{-i+1,j,0} - N_{-i-1,j,0}$$

et

$$N_{-i,j+1,0} = N_{-i+1,j,0} + N_{-i-1,j,0};$$

donc

$$(j+1) N_{-i+1,j,0} - (j+1) N_{-i-1,j,0} = i N_{-i+1,j,0} + i N_{-i-1,j,0},$$

ou bien

$$(j+1-i) N_{-i+1,j,0} = (j+1+i) N_{-i-1,j,0}.$$

Si dans cette identité nous changeons $i-1$ en $i$, nous aurons

$$(j-i) N_{-i,j,0} = (j+2+i) N_{-i-2,j,0}. \qquad \text{C. Q. F. D.}$$

*Corollaire I.* — Nous avons vu (théorème II) que

$$j - i = 2k,$$

$k$ entier et positif. Donc en remplaçant $i$ par sa valeur, il vient

$$N_{2k-j,j,0} = \frac{j-k+1}{k} N_{2k-j-2,j,0}.$$

Si dans cette formule nous faisons successivement $k = 1, 2, 3, \ldots$ et si nous remarquons que $N_{-j,j,0} = 1$, nous aurons la série des identités

$$N_{2-j,j,0} = \frac{j}{1},$$

$$N_{4-j,j,0} = \frac{j-1}{2} N_{2-j,j,0},$$

$$N_{6-j,j,0} = \frac{j-2}{3} N_{4-j,j,0},$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$N_{2k-j,j,0} = \frac{j-k+1}{k} N_{2k-2-j,j,0},$$

d'où, en multipliant,

$$N_{2k-j,j,0} = \frac{j(j-1)(j-2)\ldots(j-k+1)}{1.2.3\ldots k},$$

c'est-à-dire le coefficient de $y^k$ dans le développement du binôme $(1+y)^j$ ou de $x^{j-2k}$ dans le développement de $\left(x+\frac{1}{x}\right)^j$.

C'est au reste ce qu'il est facile de voir directement, car on a pour ce développement un polynôme de la forme

$$\left(x+\frac{1}{x}\right)^j = x^j + H_1 x^{j-2} + H_2 x^{j-4} + \ldots + H_k x^{j-2k} + \ldots + x^{-j};$$

multiplions les deux membres par $x^{2k-j}\,du$ et intégrons de $0$ à $2\pi$, il vient

$$H_k = \frac{1}{2\pi}\int_0^{2\pi} x^{2k-j}\left(x+\frac{1}{x}\right)^j du = N_{2k-j,j,0}.$$

Ainsi les nombres de Cauchy comprennent comme cas particulier les nombres figurés, et ils permettent d'en déterminer la formule générale.

*Corollaire II.* — On arriverait par une démonstration toute semblable à la relation

$$N_{-i,0,p} = -\frac{p+2+i}{p-i} N_{-i-2,0,p},$$

d'où l'on tirerait

$$N_{2k-p,0,p} = -\frac{p-k+1}{k} N_{2k-2-p,0,p} = (-1)^k \frac{p(p-1)(p-2)\ldots(p-k+1)}{1.2.3\ldots k},$$

et l'on verrait facilement que cette quantité est le coefficient de $y^k$ dans le développement du binôme $(1-y)^p$, ou de $x^{p-2k}$ dans le développement de $\left(x - \frac{1}{x}\right)^p$.

*Corollaire III.* — Il serait maintenant facile de donner la formule générale du nombre $N_{-i,j,p}$, car on connaît les coefficients des deux développements

$$\left(x + \frac{1}{x}\right)^j = x^j + A_1 x^{j-2} + A_2 x^{j-4} + A_3 x^{j-6} + \ldots + A_k x^{j-2k} + \ldots,$$

$$\left(x - \frac{1}{x}\right)^p = x^p - B_1 x^{p-2} + B_2 x^{p-4} - B_3 x^{p-6} + \ldots \pm B_k x^{p-2k} + \ldots;$$

d'où l'on déduirait

$$x^{-i}\left(x + \frac{1}{x}\right)^j \left(x - \frac{1}{x}\right)^p = x^{j+p-i} + H_1 x^{j+p-i-2} + H_2 x^{j+p-i-4} + \ldots + H_k x^{j+p-i-2k} \ldots,$$

et si l'on a

$$j + p - i = 2k,$$

le nombre N n'est autre chose que $H_k$; donc on pourrait poser l'équation

$$N_{-i,j,p} = H_k = A_k - A_{k-1}B_1 + A_{k-2}B_2 - \ldots \pm B_k,$$

ce qui fournirait la valeur générale du nombre N.

Mais nous allons voir qu'il est inutile de calculer N par cette formule, et qu'on peut former avec la plus grande facilité des tableaux aussi étendus qu'on voudra de ces quantités, par un procédé qui permet d'éviter à coup sûr toute erreur de calcul.

3. *Construction d'une table des nombres de Cauchy.* — La table de ces nombres se composera d'autant de tables partielles qu'il y a de valeurs de $p$; et ce nombre, comme nous l'avons vu, peut recevoir les valeurs :

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \ldots$$

Nous désignerons chacun de ces tableaux par la valeur de $p$ qui lui correspond.

*Tableau où $p = 0$.*

| $p$ | $j$ | VALEURS DE $i$. | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | −10 | −9 | −8 | −7 | −6 | −5 | −4 | −3 | −2 | −1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 0 | 0 | | | | | | | | | | | 1 | | | | | | | | | | |
| | 1 | | | | | | | | | | 1 * | | 1 * | | | | | | | | | |
| | 2 | | | | | | | | | 1 | | 2 ** | | 1 | | | | | | | | |
| | 3 | | | | | | | | 1 | | 3 | | 3 | | 1 | | | | | | | |
| | 4 | | | | | | | 1 | | 4 | | 6 | | 4 | | 1 | | | | | | |
| | 5 | | | | | | 1 | | 5 | | 10 | | 10 | | 5 | | 1 | | | | | |
| | 6 | | | | | 1 | | 6 | | 15 | | 20 | | 15 | | 6 | | 1 | | | | |
| | 7 | | | | 1 | | 7 | | 21 | | 35 | | 35 | | 21 | | 7 | | 1 | | | |
| | 8 | | | 1 | | 8 | | 28 | | 56 | | 70 | | 56 | | 28 | | 8 | | 1 | | |
| | 9 | | 1 | | 9 | | 36 | | 84 | | 126 | | 126 | | 84 | | 36 | | 9 | | 1 | |
| | 10 | 1 | | 10 | | 45 | | 120 | | 210 | | 252 | | 210 | | 120 | | 45 | | 10 | | 1 |

Pour le former :

1°. J'observe que $N_{0,0,0} = 1$, puisque la somme des indices est nulle, je l'écris en tête du tableau.

2°. Si à partir de ce nombre je marche en diagonale vers la gauche, je rencontre une série de cases qui correspondent encore à une somme d'indices égale à zéro, j'y place l'unité.

3°. En partant de la case (o, o, o) j'avance en diagonale vers la droite, je dois y placer l'unité en vertu du théorème III.

4°. Actuellement il est facile de continuer indéfiniment le tableau sans crainte de se tromper; car, en vertu du théorème IV, chacun des nombres se forme en prenant la somme de celui qui est immédiatement à droite et au-dessus, et de celui qui est immédiatement à gauche et au-dessus. Ainsi, à la case marquée **, il faut mettre la somme des nombres que renferment les cases marquées *; et la règle est générale.

5°. Les cases vides correspondent à des N nuls.

*Tableau où* $p = 1$.

| $p$ | $j$ | VALEURS DE $i$. | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | − 9 | − 8 | − 7 | − 6 | − 5 | − 4 | − 3 | − 2 | − 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| **1** | 0 | | | | | | | | | 1 | | 1 | | | | | | | | |
| | 1 | | | | | | | | 1 | | 2 | | 1 | | | | | | | |
| | 2 | | | | | | | 1 | | 3 | | 3 | | 1 | | | | | | |
| | 3 | | | | | | 1 | | 4 | | 6 | | 4 | | 1 | | | | | |

6°. Au moyen du tableau qui se rapporte à $p = 0$, et en faisant usage du théorème V, il est facile de former la première ligne horizontale du tableau où $p = 1$. Cette première ligne étant écrite, le procédé qui a servi à construire le tableau précédent s'applique encore et permet de continuer ce dernier indéfiniment.

7°. La première ligne du tableau ($p = 1$) servirait de même à former la première ligne du tableau ($p = 2$), que l'on achèverait encore par le même procédé; et ainsi de suite indéfiniment.

*Remarque.* — Au lieu de faire autant de tableaux qu'il y a de valeurs de $p$, on pourrait en faire autant qu'il y a de valeurs de $j$, par des procédés analogues à ceux que nous venons d'indiquer; la difficulté

n'est pas plus grande. Les applications qu'on en veut faire règlent elles-mêmes l'argument à choisir. Le tableau $j = 0$ est particulièrement utile.

## § II. — *Généralisation des transcendantes de Bessel.*

**1.** *Définitions.* — On sait que Bessel a introduit dans la Mécanique céleste la transcendante

$$\frac{1}{2\pi}\int_0^{2\pi} x^{-i} c^{\frac{ne}{2}\left(x-\frac{1}{x}\right)}\, du,$$

où

$x = c^{u\sqrt{-1}}$,
$c =$ la base des logarithmes népériens,
$e =$ l'excentricité d'une planète,
$n =$ un nombre entier positif ou négatif.

Cette quantité n'est pas autre chose que le coefficient de $x^i$ dans le développement de

$$c^{\frac{ne}{2}\left(x-\frac{1}{x}\right)},$$

suivant les puissances de $x$. Cauchy a donné des applications nouvelles de cette transcendante, dans les Notes annexées au Mémoire de M. Le Verrier sur les inégalités de Pallas [*], et dans divers autres articles insérés aux *Comptes rendus de l'Académie des Sciences* [**]. M. Hansen de Gotha en a fait usage pour le calcul des perturbations absolues des planètes, il en a même complété les tables.

Je vais donner une légère extension à la définition de Bessel, et je formerai une transcendante dont la précédente ne sera qu'un cas particulier. On verra qu'elle fournit une solution simple de questions compliquées.

Désignons par

$$(j, n)_i$$

---

[*] *Comptes rendus de l'Académie des Sciences*, t. XX.

[**] Tome XII.

le coefficient de $x^i$ dans le développement de la fonction

$$\left(x+\frac{1}{x}\right)^j c^{\frac{ne}{2}\left(x-\frac{1}{x}\right)}$$

suivant les puissances de $x$; en d'autres termes, posons

$$(j,n)_i = \frac{1}{2\pi}\int_0^{2\pi} x^{-i}\left(x+\frac{1}{x}\right)^j c^{\frac{ne}{2}\left(x-\frac{1}{x}\right)}\,du,$$

la transcendante de Bessel se déduira de celle-ci en faisant $j=0$.

2. *Propriétés de la transcendante* $(j,n)_i$. — Cette transcendante se lie intimement aux nombres $N_{-i,j,p}$, comme nous allons le faire voir, et ses propriétés découlent immédiatement des propriétés de ces nombres.

Théorème I. — *Le calcul de la transcendante* $(j,n)_i$ *se ramène au calcul de l'exponentielle* $c^{\frac{ne}{2}}$, *au moyen des nombres de Cauchy.*

En effet, nous avons

$$C^{\frac{ne}{2}\left(x-\frac{1}{x}\right)} = \sum_{0}^{\infty}{}_p \frac{\left(\frac{ne}{2}\right)^p}{1.2.3\ldots p}\left(x-\frac{1}{x}\right)^p,$$

donc

$$(j,n)_i = \sum_{0}^{\infty}{}_p \frac{\left(\frac{ne}{2}\right)^p}{1.2.3\ldots p}\,\frac{1}{2\pi}\int_0^{2\pi} x^{-i}\left(x+\frac{1}{x}\right)^j\left(x-\frac{1}{x}\right)^p du,$$

ou bien

$$(j,n)_i = \sum_{0}^{\infty}{}_p \frac{\left(\frac{ne}{2}\right)^p}{1.2.3\ldots p}\,N_{-i,j,p}.$$

La transcendante de Bessel en particulier sera donnée par l'équa-

tion

$$(0,n)_i = \sum_{0}^{\infty}{}_p \frac{\left(\frac{ne}{2}\right)^p}{1.2.3\ldots p} N_{-i.0.p}.$$

Ces formules montrent, qu'une fois construites les tables des nombres N, le calcul des transcendantes n'est pas plus difficile que celui qui conduit à la détermination de $c^{\frac{ne}{2}}$, seulement la série est moins convergente.

Théorème II. — *La transcendante $(j, n)_i$ peut se calculer au moyen des transcendantes $(j-1, n)_i$, par la formule*

$$(j,n)_i = (j-1,n)_{i-1} + (j-1,n)_{i+1}.$$

C'est une conséquence du théorème IV du § I.

Théorème III. — *Si $i$ change de signe, $(j, n)_i$ garde la même valeur numérique, mais il change de signe si $j-i$ est impair.*

Théorème IV. — *Si $n$ change de signe, $(j, n)_i$ garde la même valeur numérique, mais il change de signe si $j-i$ est impair.*

Théorème V. — *$(j, n)_i$ reste le même quand $i$ et $n$ changent tous deux de signe.*

On trouvera sans peine les démonstrations de ces théorèmes à l'aide des propriétés des nombres N.

Théorème VI. — *On a entre $(1,n)_i$ et $(0,n)_i$ la relation*

$$(1,n)_i = \frac{i}{\left(\frac{ne}{2}\right)}(0,n)_i.$$

On peut déduire cette relation de l'intégration par parties appliquée directement à l'équation qui définit la transcendante; mais on y arrive plus simplement encore au moyen des propriétés des nombres de

Cauchy. On a

$$(1, n)_i = \sum_{0}^{\infty} {}_p \frac{\left(\frac{ne}{2}\right)^p}{1.2\ldots p} \mathrm{N}_{-i,1,p}.$$

Or (théorème VI, § I)

$$\mathrm{N}_{-i,1,p} = \frac{i}{p+1} \mathrm{N}_{-i,0,p+1};$$

donc

$$(1, n)_i = \frac{i}{\left(\frac{ne}{2}\right)} \sum_{0}^{\infty} {}_p \frac{\left(\frac{ne}{2}\right)^{p+1}}{1.2.3\ldots p(p+1)} \mathrm{N}_{-i,0,p+1},$$

ou bien

$$(1, n)_i = \frac{i}{\left(\frac{ne}{2}\right)} (0, n)_i.$$

Théorème VII. — *Il existe entre trois transcendantes consécutives, relativement aux valeurs de* $j$, *la relation*

$$(j+2, n)_i = \frac{i}{\left(\frac{ne}{2}\right)} (j+1, n)_i - \frac{j+1}{\left(\frac{ne}{2}\right)} [(j, n)_{i-1} - (j, n)_{i+1}].$$

En effet, nous avons

$$(j, n)_{i-1} - (j, n)_{i+1} = \sum_{0}^{\infty} {}_p \frac{\left(\frac{ne}{2}\right)^p}{1.2.3\ldots p} (\mathrm{N}_{-i+1,j,p} - \mathrm{N}_{-i-1,j,p})$$

$$= \sum_{0}^{\infty} {}_p \frac{\left(\frac{ne}{2}\right)^p}{1.2.3\ldots p} \mathrm{N}_{-i,j,p+1}.$$

Or, en vertu du théorème VI du § I,

$$\mathrm{N}_{-i,j,p+1} = \frac{i}{j+1} \mathrm{N}_{-i,j+1,p} - \frac{p}{j+1} \mathrm{N}_{-i,j+2,p-1};$$

donc

$$(j, n)_{i-1} - (j, n)_{i+1} = \frac{i}{j+1} (j+1, n)_i - \frac{\left(\frac{ne}{2}\right)}{j+1} (j+2, n)_i,$$

ou bien

$$(j+2,n)_i = \frac{i}{\left(\frac{ne}{2}\right)}(j+1,n)_i - \frac{j+1}{\left(\frac{ne}{2}\right)}[(j,n)_{i-1} - (j,n)_{i+1}],$$

C. Q. F. D.

Théorème VIII. — *Une transcendante de Bessel peut se calculer, au moyen des précédentes, par la formule*

$$(0,n)_{i+1} = \frac{i}{\left(\frac{ne}{2}\right)}(0,n)_i - (0,n)_{i-1}.$$

En effet, le théorème II donne

$$(1,n)_i = (0,n)_{i-1} + (0,n)_{i+1};$$

d'autre part, le théorème VI donne

$$(1,n)_i = \frac{i}{\left(\frac{ne}{2}\right)}(0,n)_i;$$

donc

$$\frac{i}{\left(\frac{ne}{2}\right)}(0,n)_i = (0,n)_{i-1} + (0,n)_{i+1},$$

ce qui démontre le théorème énoncé.

*Remarque.* — Les théorèmes qui précèdent font voir que le calcul des transcendantes généralisées se ramène, si l'on veut, à celui des transcendantes de Bessel; ils fournissent d'ailleurs des relations d'identité précieuses pour vérifier leur exactitude.

## § III. — *Applications des nombres de Cauchy et des transcendantes de Bessel au problème de Képler.*

1. Dans une Note présentée à l'Académie [*], j'ai montré avec

[*] *Comptes rendus de l'Académie des Sciences*, t. XXXVIII, p. 807.

quelle élégance l'emploi des nombres N résolvait le problème de Képler; je vais résumer ici ce travail, et y ajouter les perfectionnements qui résultent de l'introduction des nouvelles transcendantes.

2. *Développement de l'anomalie excentrique.* — L'anomalie excentrique $u$ est liée à l'anomalie moyenne T par l'équation transcendante

$$T = u - e \sin u.$$

Il s'agit de trouver $u$ en fonction de T.

On peut développer $u$ suivant les puissances de l'exponentielle imaginaire $c^{T\sqrt{-1}}$; posons

$$u - T = \sum_{-\infty}^{\infty}{}_i A_i c^{iT\sqrt{-1}}.$$

Cauchy a démontré [*] que pour obtenir $A_i$, coefficient de $c^{iT\sqrt{-1}}$, il suffit de chercher le coefficient de $x^i = c^{iu\sqrt{-1}}$ dans le développement de la même fonction multipliée par

$$(1 - e\cos u)\, c^{\frac{ie}{2}\left(x - \frac{1}{x}\right)} = \left[1 - \frac{e}{2}\left(x + \frac{1}{x}\right)\right] c^{\frac{ie}{2}\left(x - \frac{1}{x}\right)},$$

suivant les puissances de $x$. Appliquons ce théorème, facile d'ailleurs à démontrer, nous aurons

$$A_i = \frac{1}{2\pi}\int_0^{2\pi} x^{-i} e \sin u \left[1 - \frac{e}{2}\left(x + \frac{1}{x}\right)\right] c^{\frac{ie}{2}\left(x - \frac{1}{x}\right)} du.$$

En développant, nous trouvons

$$A_i = \frac{e}{2\sqrt{-1}}\left[(0, i)_{i-1} - (0, i)_{i+1} - \frac{e}{2}(1, i)_{i-1} + \frac{e}{2}(1, i)_{i+1}\right].$$

---

[*] *Comptes rendus de l'Académie des Sciences*, t. XII, p. 85.

et si nous invoquons les théorèmes VI et VIII du § I, nous obenons

$$\mathrm{A}_i = \frac{e}{2i\sqrt{-1}}(1, i)_i,$$

ou encore

$$\mathrm{A}_i = \frac{1}{i\sqrt{-1}}(0, i)_i.$$

Le terme conjugué du développement sera

$$\mathrm{A}_{-i} = -\frac{1}{i\sqrt{-1}}(0, i)_i = -\mathrm{A}_i,$$

donc la réunion de ces deux termes donnera pour terme général de $u - \mathrm{T}$

$$\frac{2}{i}(0, i)_i \sin i\mathrm{T}.$$

Si l'on veut se dispenser de l'emploi des transcendantes de Bessel, on introduira leur valeur, et le terme général du même développement deviendra

$$\frac{2}{i}\sin i\mathrm{T}\sum_{0}^{\infty}{}_p \frac{\left(\frac{ie}{2}\right)^p}{1.2\ldots p}\mathrm{N}_{-i,0,p}.$$

C'est sous cette forme que nous l'avons présenté autrefois.

**5.** *Développement du rayon vecteur.* — Le rayon vecteur est donné par la formule

$$r = a(1 - e\cos u),$$

il s'agit de trouver sa valeur en fonction de l'anomalie moyenne T. Posons

$$\frac{r}{a} = \sum_{-\infty}^{\infty}{}_i \mathrm{B}_i c^{i\mathrm{T}\sqrt{-1}}$$

il viendra en vertu du théorème de Cauchy

$$\mathrm{B}_i = \frac{1}{2\pi}\int_0^{2\pi} x^{-i}\left[1 - \frac{e}{2}\left(x + \frac{1}{x}\right)\right]^2 c^{\frac{ie}{2}\left(x - \frac{1}{x}\right)} du$$

et en développant

$$B_i = (0, i)_i - e(1, i)_i + \frac{e^2}{4}(2, i)_i.$$

Si maintenant nous invoquons les théorèmes II et VI, nous ramènerons tout aux transcendantes de Bessel, et il viendra simplement

$$B_i = -\frac{e}{2i}[(0, i)_{i-1} - (0, i)_{i+1}].$$

Le terme conjugué $B_{-i}$ est égal à $B_i$, en réunissant ces deux termes nous avons pour le terme général de $\frac{r}{a}$

$$-\frac{e}{i}[(0, i)_{i-1} - (0, i)_{i+1}] \cos i\mathrm{T}.$$

Si l'on veut se dispenser de l'emploi des transcendantes, on les remplacera par leur valeur en fonction des nombres de Cauchy, et l'on obtiendra pour la formule du terme général de $\frac{r}{a}$ l'expression

$$-\frac{e}{i}\cos i\mathrm{T}\sum_0^\infty {}_p \frac{\left(\frac{ie}{2}\right)^p}{1.2.3\ldots p}[\mathrm{N}_{-i+1,0,p} - \mathrm{N}_{-i-1,0,p}],$$

ou bien encore

$$-\frac{e}{i}\cos i\mathrm{T}\sum_0^\infty {}_p \frac{\left(\frac{ie}{2}\right)^p}{1.2.3\ldots p}\mathrm{N}_{-i,0,p+1}.$$

Quant à $B_0$, on le déduit directement de la formule primitive qui donne $B_i$ par l'intégrale définie, et l'on trouve sans peine qu'il est égal au terme indépendant de $x$ dans le développement du carré

$$\left[1 - \frac{e}{2}\left(x + \frac{1}{x}\right)\right]^2,$$

donc

$$B_0 = 1 + \frac{e^2}{2}.$$

4. *Développement du logarithme népérien du rayon vecteur.* — Désignons par $B'_i$ le coefficient de l'exponentielle

$$c^{i\mathrm{T}\sqrt{-1}},$$

dans ce développement, nous aurons

$$B'_i = \frac{1}{2\pi}\int_0^{2\pi} c^{-i\mathrm{T}\sqrt{-1}}\, l\frac{r}{a}\,.\,d\mathrm{T};$$

remplaçons $\frac{r}{a}$ par sa valeur en $u$; intégrons par parties, nous aurons

$$B'_i = \frac{e}{i\sqrt{-1}}\,\frac{1}{2\pi}\int_0^{2\pi} c^{-i\mathrm{T}\sqrt{-1}}\,\frac{\sin u}{1 - e\cos u}\,du;$$

développons $(1 - e\cos u)^{-1}$, il viendra

$$\left[1 - \frac{e}{2}\left(x + \frac{1}{x}\right)\right]^{-1} = \sum_0^{\infty}{}_j \left(\frac{e}{2}\right)^j \left(x + \frac{1}{x}\right)^j,$$

puis observons que

$$c^{-i\mathrm{T}\sqrt{-1}} = c^{-iu\sqrt{-1}}\quad c^{\frac{ie}{2}\left(x - \frac{1}{x}\right)} = x^{-i}\, c^{\frac{ie}{2}\left(x - \frac{1}{x}\right)},$$

nous aurons

$$B'_i = -\frac{e}{2i}\sum_0^{\infty}{}_j \left(\frac{e}{2}\right)^j \cdot \frac{1}{2\pi}\int_0^{2\pi} x^{-i}\left(x - \frac{1}{x}\right)\left(x + \frac{1}{x}\right)^j c^{\frac{ie}{2}\left(x - \frac{1}{x}\right)} du.$$

A l'aide des transcendantes de Bessel généralisées, cette formule devient simplement

$$B'_i = -\frac{e}{2i}\sum_0^{\infty}{}_j \left(\frac{e}{2}\right)^j \left[(j,i)_{i-1} - (j,i)_{i+1}\right];$$

de là nous conclurons

$$B'_{-i} = \frac{e}{2i}\sum_{1}^{\infty}{}_j \left(\frac{e}{2}\right)^j [(j,i)_{i+1} - (j,i)_{i-1}] = B'_i;$$

donc, en réunissant les deux termes conjugués, nous aurons pour le terme général du développement de $l\frac{r}{a}$

$$-\frac{e}{i}\sum_{0}^{\infty}{}_j \left(\frac{e}{2}\right)^j [(j,i)_{i-1} - (j,i)_{i+1}] \cos i\mathrm{T}.$$

Si l'on veut éviter l'emploi des transcendantes, on substituera leurs valeurs et le terme général prendra la forme

$$-\frac{e}{i}\sum_{0}^{\infty}{}_j \sum_{0}^{\infty}{}_p \left(\frac{e}{2}\right)^j \frac{\left(\frac{ie}{2}\right)^p}{1.2\ldots p} \mathrm{N}_{-i,j,p+1} \cos i\mathrm{T}.$$

Pour trouver $B'_0$, j'observe qu'il est d'abord donné par la formule

$$B'_0 = \frac{1}{2\pi}\int_0^{2\pi} l(1 - e\cos u).d\mathrm{T}.$$

Prenons $u$ pour variable indépendante, et développons le logarithme en série par la formule

$$l(1 - e\cos u) = -\sum_{1}^{\infty}{}_j \frac{1}{j}\left(\frac{e}{2}\right)^j \left(x + \frac{1}{x}\right)^j,$$

nous obtiendrons

$$B'_0 = -\sum_{1}^{\infty}{}_j \frac{1}{j}\left(\frac{e}{2}\right)^j \frac{1}{2\pi}\int_0^{2\pi}\left[1 - \frac{e}{2}\left(x + \frac{1}{x}\right)\right]\left(x + \frac{1}{x}\right)^j du,$$

et en introduisant les nombres de Cauchy,

$$B'_0 = -\sum_{1}^{\infty}{}_j \frac{1}{j}\left(\frac{e}{2}\right)^j \left[\mathrm{N}_{0,j,0} - \frac{e}{2}\mathrm{N}_{0,j+1,0}\right].$$

5. *Développement de l'équation du centre.* — La recherche du terme général du développement de l'équation du centre est un problème regardé comme difficile. Bessel et Poisson s'en sont occupés; les recherches de Bessel datent de 1816, celles de Poisson se trouvent dans les *Additions à la Connaissance des Temps* pour 1825 et 1826. M. Lefort a résolu complétement le problème dans un Mémoire qui fait partie du t. XI du *Journal de Mathématiques* de M. Liouville. Toutefois la formule de M. Lefort est si longue, qu'il paraît impossible d'en faire usage; nous allons voir que l'introduction des nombres N et des transcendantes $(j, n)_i$ lui donne une forme extrêmement simple.

Désignons par $w$ l'anomalie vraie, l'équation du centre sera $w - \mathrm{T}$; posons

$$w - \mathrm{T} = \sum_{-\infty}^{\infty}{}_i \, \mathrm{C}_i c^{i\mathrm{T}\sqrt{-1}},$$

il vient

$$\mathrm{C}_i = \frac{1}{2\pi}\int_0^{2\pi} c^{-i\mathrm{T}\sqrt{-1}}(w - \mathrm{T})\,d\mathrm{T}.$$

Intégrons par parties, nous trouverons simplement

$$\mathrm{C}_i = \frac{1}{i\sqrt{-1}}\,\frac{1}{2\pi}\int_0^{2\pi} c^{-i\mathrm{T}\sqrt{-1}}\,dw.$$

Introduisons partout l'anomalie excentrique $u$ au moyen de la formule

$$\cos w = \frac{\cos u - e}{1 - e\cos u};$$

il viendra, en posant

$$f = \sqrt{i - e^2}$$

et nommant $j$ un nombre entier,

$$\mathrm{C}_i = \frac{f}{i\sqrt{-1}}\sum_0^{\infty}{}_j\left(\frac{e}{2}\right)^j \frac{1}{2\pi}\int_0^{2\pi} x^{-i}\left(x + \frac{1}{x}\right)^j c^{\frac{ie}{2}\left(x - \frac{1}{x}\right)}\,du,$$

ou bien

$$\mathrm{C}_i = \frac{f}{i\sqrt{-1}}\sum_0^{\infty}{}_j\left(\frac{e}{2}\right)^j (j, i)_i.$$

Le terme conjugué est

$$C_{-i} = -\frac{f}{i\sqrt{-1}}\sum_{0}^{\infty}{}_j\left(\frac{e}{2}\right)^j(j,i)_i = -C_i;$$

donc le terme général de l'équation du centre qui résulte de l'addition des deux termes conjugués sera

$$\frac{2f}{i}\sin i\mathrm{T}\sum_{0}^{\infty}{}_j\left(\frac{e}{2}\right)^j(j,i)_i,$$

expression extrêmement simple si on la compare à celle que M. Lefort a donnée à la page 151 du tome XI.

Si l'on veut éviter l'emploi des transcendantes, on substituera leur valeur en fonction des nombres de Cauchy, et l'on trouvera la formule à somme double

$$\frac{2f}{i}\sin i\mathrm{T}\sum_{0}^{\infty}{}_j\sum_{0}^{\infty}{}_p\left(\frac{e}{2}\right)^j\frac{\left(\frac{ie}{2}\right)^p}{1.2.3\ldots p}\mathrm{N}_{-i,j,p}.$$

6. *Développement de* $\frac{a}{r}$. — Ce développement se trouve indiqué à la page 30 du Mémoire de M. Hansen sur la détermination des perturbations absolues (traduction de M. Mauvais); on l'effectue encore avec la plus grande facilité au moyen du procédé que nous avons employé pour les fonctions précédentes.

Posons

$$\frac{a}{r} = \sum_{-\infty}^{\infty}{}_i \mathrm{D}_i c^{i\mathrm{T}\sqrt{-1}},$$

il viendra

$$\mathrm{D}_i = \frac{1}{2\pi}\int_0^{2\pi}(1-e\cos u)^{-1}c^{-i\mathrm{T}\sqrt{-1}}\,d\mathrm{T},$$

ou bien

$$\mathrm{D}_i = \frac{1}{2\pi}\int_0^{2\pi}x^{-i}c^{\frac{ie}{2}\left(x-\frac{1}{x}\right)}\,du;$$

donc

$$D_i = (o, i)_i,$$

et comme

$$D_{-i} = (o, i)_i = D_i,$$

le terme général du développement de $\frac{a}{r}$ qui résulte de la somme des deux termes conjugués

$$D_i c^{iT\sqrt{-1}}, \quad D_{-i} c^{-iT\sqrt{-1}}$$

sera

$$2 \cos iT.(o, i)_i,$$

ou bien

$$2 \cos iT \sum_{0}^{\infty}{}_p \frac{\left(\frac{ie}{2}\right)^p}{1.2.3\ldots p} N_{-i, o, p}.$$

Quant au terme $D_0$, on trouve qu'il est égal à l'unité. Cela résulte immédiatement de l'intégration qui en donne la valeur.

7. Nous pourrions multiplier encore les applications des transcendantes de Bessel et des nombres N; mais ce que nous venons d'exposer et les Notes de Cauchy (*Comptes rendus de l'Académie*, t. XIII, p. 682 et 850) montrent suffisamment toute leur importance en mécanique céleste. Nous avons pu, à l'aide de ces quantités, simplifier notablement les belles méthodes d'interpolation de Cauchy (*Comptes rendus de l'Académie*, t. XX, p. 769). Nous réservons pour un autre Mémoire l'exposition détaillée de cette nouvelle application.

# NOUVEAU THÉORÈME

## CONCERNANT LES NOMBRES PREMIERS DE LA FORME $8\mu+1$;

**Par M. J. LIOUVILLE.**

Étant donné un nombre premier $m$ de la forme $8\mu+1$, je pose de toutes les manières possibles l'équation

$$m = 2p^{4\alpha+1}x^2 + q^{4\beta+1}y^2,$$

$x$ et $y$ étant des entiers impairs et $p$, $q$ des nombres premiers de la forme $8\nu+3$, $p$ non diviseur de $x$, $q$ non diviseur de $y$ : j'admets pour $\alpha$ et pour $\beta$ la valeur zéro. On demande une règle facile qui dise à priori si le nombre N des décompositions de $m$ sous la forme indiquée est pair ou impair.

La réponse que nous ferons à cette question est entièrement semblable à celle que nous avons faite (dans le cahier de *janvier*) à l'occasion d'une équation bien différente pourtant de celle qui nous occupe aujourd'hui : « Formez l'équation, en nombres entiers,

$$m = a^2 + 8b^2,$$

» qui a toujours lieu, d'une seule manière, pour un nombre premier
» $m$ de la forme $8\mu+1$; N sera pair si $b$ est pair, mais impair si $b$
» est impair. »

En d'autres termes, on a toujours

$$\mathrm{N} \equiv b \pmod{2}.$$

Ainsi, pour

$$m = 17 = 3^2 + 8.1^2,$$

on a $b=1$, donc N impair, et en effet il n'existe qu'une seule décom-

position du genre demandé, celle que fournit l'équation

$$17 = 2.3.1^2 + 11.1^2.$$

Au contraire, pour

$$m = 41 = 3^2 + 8.2^2,$$

on a $b = 2$, donc N pair; et cela est exact encore puisque les décompositions canoniques sont ici au nombre de deux, savoir

$$41 = 2.11.1^2 + 19.1^2$$

et

$$41 = 2.19.1^2 + 3.1^2.$$

Nous ne pousserons pas plus loin les exemples.

NOUVELLE THÉORIE

DES

# FONCTIONS DE VARIABLES IMAGINAIRES;

PAR M. MAXIMILIEN MARIE,
Ancien élève de l'École Polytechnique.

## TROISIÈME PARTIE.

DE LA MARCHE DES VALEURS D'UNE FONCTION IMPLICITE DÉFINIE PAR UNE ÉQUATION ALGÉBRIQUE.
(Suite.)

## CHAPITRE VII.

*De la série de Taylor.* (Suite.)

APPLICATIONS.

**107.** Soit d'abord l'équation

$$y^2 = 2px:$$

$x_0 = \alpha_0 + \beta_0\sqrt{-1}$ désignant l'abscisse du point de départ, et $x_1 = \alpha_1 + \beta_1\sqrt{-1}$ celle d'un point de la région de convergence, $\alpha_1$ et $\beta_1$ devront satisfaire à la condition

$$(\alpha_1 - \alpha_0)^2 + (\beta_1 - \beta_0)^2 < \alpha_0^2 + \beta_0^2,$$

ou

$$\alpha_1^2 - 2\alpha_0\alpha_1 + \beta_1^2 - 2\beta_1\beta_0 < 0;$$

pour que le point mobile puisse passer sur la conjuguée dangereuse

$C = \infty$, il faudra donc que l'on puisse trouver des valeurs négatives de $\alpha$, telles que

$$\alpha^2 - 2\alpha\alpha_0 < 0,$$

c'est-à-dire qu'il faudra que $\alpha_0$ soit lui-même négatif.

Supposons d'abord $\alpha_0$ positif : le point mobile n'ayant pu passer sur la conjuguée $C = \infty$, la caractéristique du point final aura le signe de celle du point initial ; et comme les caractéristiques de deux points ayant même abscisse sont toujours de signes contraires, il n'y aura aucun doute sur la valeur de $y$, qui se sera développée suivant la série.

Supposons maintenant $\alpha_0$ négatif : le point mobile ne pourra pas dans ce cas passer sur la courbe réelle, car il n'existera pas de valeurs positives de $\alpha$ satisfaisant à l'inégalité

$$\alpha^2 - 2\alpha_0\alpha < 0;$$

$\beta'$ ne pourra donc pas changer de signe ; et si $\beta$ en a changé, dans le passage de $x_0$ à $x_1$, le point $[x, y]$ aura certainement traversé la conjuguée dangereuse, tandis que dans le cas contraire il ne l'aura pas traversée, ou l'aura traversée un nombre pair de fois, ce qui revient au même.

La caractéristique du point final aura donc, ou non, le signe de la caractéristique du point initial, suivant que $\beta_0$ et $\beta_1$ seront de même signe ou de signes contraires.

On construirait très-aisément, si on le voulait, la limite de la région de convergence : cette courbe passerait, dans tous les cas, par le point dangereux, et y toucherait la courbe réelle et la conjuguée $C = \infty$ ; elle n'aurait d'ailleurs que ce point commun, soit avec la courbe réelle, soit avec la conjuguée $C = \infty$, suivant que $\alpha_0$ serait négatif ou positif. Dans le premier cas, les deux points d'une même conjuguée, situés sur la limite de la région de convergence, appartiendraient toujours à des branches inférieures ou supérieures, suivant que le point de départ $[x_0, y_0]$ serait lui-même sur une branche inférieure ou sur une branche supérieure ; dans le second, les points de la limite, pour lesquels $\beta$ serait de même signe que $\beta_0$, appartiendraient à des branches de même nature que celle où se trouvait le point de départ ; et les autres à des branches

de nature contraire. Dans ce dernier cas, la région de convergence serait repliée sur elle-même.

**108.** Soit maintenant l'équation

$$a^2 y^2 + b^2 x^2 = a^2 b^2:$$

ce sera le sommet de droite A, ou le sommet de gauche A', qui limitera la région de convergence, suivant que

$$\beta_0^2 + (\alpha_0 - a)^2 \lessgtr \beta_0^2 + (\alpha_0 + a)^2,$$

c'est-à-dire suivant que $\alpha_0$ sera positif ou négatif.

Il est facile d'interpréter ce résultat :

La partie réelle de l'abscisse d'un point du lieu ne passe par zéro que lorsque le point lui-même passe sur la conjuguée C = o, c'est-à-dire sur l'hyperbole qui touche l'ellipse en ses sommets B et B' placés sur l'axe des $y$. Du reste, il est évident que la partie imaginaire de $x$ est positive ou négative suivant que le point appartient à une branche d'hyperbole tangente à l'ellipse en un point de l'arc BAB' ou en un point de l'arc BA'B'.

On voit donc que le point dangereux qui limite la région de convergence est toujours le sommet le plus proche du point où la branche de conjuguée, qui contient le point de départ, touche l'ellipse.

Supposons $\alpha_0$ positif : le point $[x, y]$ pourra ou non passer sur la conjuguée dangereuse $C = \infty$, sans sortir de la région de convergence, suivant qu'on pourra ou non satisfaire à la condition

$$(\alpha - \alpha_0)^2 + \beta_0^2 < (\alpha_0 - a)^2 + \beta_0^2$$

par des valeurs positives de $\alpha$ plus grandes que $a$.

Cette condition se réduit à $\alpha_0 > a$; si donc $\alpha_0$ est moindre que $a$, le point $[x, y]$ ne pouvant, sans sortir de la région de convergence, passer sur la conjuguée $C = \infty$, la caractéristique du point final aura le signe de la caractéristique du point initial ou un signe contraire, suivant que, dans l'intervalle, le point mobile n'aura pas ou aura traversé la conjuguée C = o, c'est-à-dire suivant que $\alpha_1$ et $\alpha_0$ seront de même signe ou de signes contraires. Comme du reste les caractéristi-

ques de deux points ayant même abscisse sont toujours de signes contraires, il ne restera aucun doute sur celle des valeurs de $y$ qui se sera développée par la série de Taylor.

Si la valeur finale de $x$ était réelle et moindre que $a$, les valeurs finales de $y$ seraient aussi réelles, mais le point d'arrivée serait évidemment sur la branche d'ellipse qui contiendrait le point de contact de la branche d'hyperbole où se trouvait le point de départ.

Supposons maintenant $\alpha_0 > a$: pour que le point mobile $[x, y]$ pût passer sur la courbe réelle, il faudrait qu'on pût satisfaire à la condition

$$(\alpha - \alpha_0)^2 + \beta_0^2 < (\alpha_0 - a)^2 + \beta_0^2$$

au moyen de valeurs de $\alpha$ comprises entre $-a$ et $+a$; or cette condition se réduit à

$$(\alpha - a)(\alpha + a - 2\alpha_0) < 0,$$

elle ne peut donc être satisfaite; ainsi la limite de la région de convergence touchera seulement la courbe réelle au sommet A.

Dans ce cas de $\alpha_0 < a$, la caractéristique pourra changer de signe en passant par $\infty$ ou par 0, car le point $[x, y]$ pourra traverser la conjuguée $C = 0$ s'il existe pour $\beta$ des valeurs satisfaisant à la condition

$$\alpha_0^2 + (\beta - \beta_0)^2 < (\alpha_0 - a)^2 + \beta_0^2,$$

ou

$$\beta^2 - 2\beta\beta_0 < a^2 - 2a\alpha_0.$$

Il n'y a à cette condition aucun empêchement général; par conséquent, suivant que $\alpha_1\beta_1$ et $\alpha_0\beta_0$ seront de même signe ou de signes contraires, les caractéristiques des deux points extrêmes seront aussi de même signe ou de signes contraires.

**109.** J'ai voulu, dans ce qui précède, pour plus de précision, déterminer le signe de la caractéristique du point d'arrivée; mais il est évident que la question ne l'exigeait pas, car deux points qui ont même abscisse, étant toujours séparés par la conjuguée dangereuse, il suffisait pour choisir la valeur finale de $y$ de savoir si le point mobile,

pendant son mouvement, avait ou non traversé cette conjuguée dangereuse.

J'abrégerai dans les exemples suivants.

L'équation

$$a^2 y^2 + b^2 x^2 = -a^2 b^2$$

se discutera comme la précédente; cependant elle offrira quelques particularités nouvelles, parce que l'enveloppe des conjuguées ne sera plus réelle.

La région de convergence sera limitée au sommet de droite A, ou au sommet de gauche A′ de l'enveloppe, selon que

$$\alpha_0^2 + (\beta_0 - a)^2 \lessgtr \alpha_0^2 + (\beta_0 + a)^2,$$

ou que $\beta_0$ sera positif ou négatif.

Or la partie imaginaire de l'abscisse d'un point du lieu ne passe par zéro que lorsque le point lui-même passe sur la conjuguée $C = \infty$ qui touche l'enveloppe en ses sommets placés sur l'axe des $y$ : on conclut de là, comme dans le cas précédent, que le point dangereux qui limite la région de convergence est toujours le sommet le plus proche du point où la branche, qui contient le point de départ, touche l'enveloppe.

Supposons $\beta_0$ positif: le point $[x, y]$ pourra ou non passer sur la conjuguée dangereuse $C = 0$, suivant qu'on pourra ou non trouver pour $\beta$ des valeurs positives et plus grandes que $a$, qui satisfassent à la condition

$$\alpha_0^2 + (\beta - \beta_0)^2 < \alpha_0^2 + (\beta_0 - a)^2.$$

Cette condition se réduit à

$$(\beta - a)(\beta + a - 2\beta_0) < 0;$$

le point mobile pourra donc ou non passer sur la conjuguée dangereuse, suivant que $\beta_0$ sera plus grand ou plus petit que $a$.

Au reste, on verrait, comme précédemment, que lorsque le point $[x, y]$ peut passer sur la conjuguée dangereuse $C = 0$, il ne peut parvenir à l'enveloppe et réciproquement, puisque la condition est la

même dans les deux cas,

$$(\beta - a)(\beta + a - 2\beta_0) < 0,$$

mais avec les hypothèses contraires $\beta < a$ et $\beta > a$. D'un autre côté le point $[x, y]$ pourra ou non passer sur la conjuguée $C = \infty$, suivant qu'on pourra ou non trouver pour $\alpha$ des valeurs satisfaisant à la condition

$$(\alpha - \alpha_0)^2 + \beta_0^2 < \alpha_0^2 + (\beta_0 - a)^2,$$

ou

$$\alpha^2 - 2\alpha\alpha_0 < a^2 - 2a\beta_0.$$

Cela posé :

Si $\beta_0$ est plus grand que $a$, le point $[x, y]$ pourra passer sur la conjuguée dangereuse $C = 0$, et il y aura ou non passé, suivant que $\alpha_1$ et $\alpha_0$ seront de signes contraires ou de même signe ; de même, il aura ou non traversé la conjuguée $C = \infty$, suivant que $\beta_0$ et $\beta_1$ seront de signes contraires ou de même signe ; la caractéristique du point final sera donc de même signe que celle du point initial, ou aura un signe contraire, suivant que

$$\alpha_1 \alpha_0 \beta_1 \beta_0$$

sera positif ou négatif.

Si, au contraire, $\beta_0$ est moindre que $a$, suivant que $\beta_1$ et $\beta_0$ seront de signes contraires ou de même signe, le point $[x, y]$ aura ou non traversé la conjuguée $C = \infty$, de sorte que les caractéristiques du point initial et du point final seront alors de signes contraires ou de même signe ; tandis que, suivant que $\alpha_1$ et $\alpha_0$ seront de signes contraires ou de même signe, le point mobile ayant ou non passé sur l'enveloppe, le point final et le point initial seront, sur leurs conjuguées respectives, de côtés opposés ou du même côté par rapport aux points où ces conjuguées touchent l'enveloppe, sans qu'il en puisse d'ailleurs résulter de changement de signe dans la caractéristique : ce serait la partie imaginaire de $\frac{dy}{dx}$ qui changerait de signe avec $\alpha$, de sorte qu'on eût pu proposer de reconnaître, parmi les deux valeurs finales de $y$, celle qui se serait développée par la série de Taylor, au signe de la partie imaginaire de la valeur qu'elle devait faire prendre à $\frac{dy}{dx}$.

**110.** Prenons encore l'équation

$$a^2 y^2 - b^2 x^2 = -a^2 b^2.$$

La région de convergence sera bornée au sommet de droite ou au sommet de gauche, suivant que

$$(\alpha_0 - a)^2 + \beta_0^2 \lessgtr (\alpha_0 + a)^2 + \beta_0^2,$$

c'est-à-dire suivant que $\alpha_0$ sera positif ou négatif.

Or, quand on suit une même conjuguée en allant de droite à gauche, $\alpha$ est d'abord positif aux environs du point de contact de la conjuguée avec la branche droite de l'hyperbole ; il est négatif aux environs du point de contact de gauche, et il s'annule aux extrémités du diamètre conjugué de celui qui passe par les deux points de contact.

Sur quelque conjuguée que se trouve le point initial, le sommet où se trouve bornée la région de convergence est donc toujours celui qui appartient à la branche de l'hyperbole réelle qui passe par l'extrémité du quadrant (oblique) de conjuguée sur lequel se trouve le point initial.

**111.** S'il s'agissait de l'équation

$$a^2 y^2 - b^2 x^2 = a^2 b^2,$$

les points dangereux seraient les sommets de l'enveloppe imaginaire des conjuguées.

La région de convergence serait limitée au sommet de droite ou au sommet de gauche suivant que

$$\alpha_0^2 + (\beta_0 - a)^2 \lessgtr \alpha_0^2 + (\beta_0 + a)^2,$$

ou que $\beta_0$ serait positif ou négatif.

Cette condition s'interpréterait comme dans le cas précédent.

On achèverait dans ces deux derniers exemples la détermination de la valeur finale de $y$ comme dans les deux précédents.

**112.** L'équation

$$y^n = (a + x)^m.$$

qu'on ramène par une transformation de variables à

$$y^n = (1 + x)^m,$$

où l'on peut supposer que $x$ parte de 0, est, je crois, la seule qu'on ait jusqu'ici discutée au point de vue qui nous occupe.

Le point dangereux est $x = -1$, $y = 0$, de sorte que la seule conjuguée dangereuse est la conjuguée $C = \infty$ : les branches de cette conjuguée sont représentées, du côté des $x$ plus grands que $-1$ par les équations

$$y = \rho^{\frac{m}{n}} \left( \cos \frac{2k\pi}{n} + \sqrt{-1} \sin \frac{2k\pi}{n} \right)$$

et du côté des $x$ moindres que $-1$ par

$$y = \rho^{\frac{m}{n}} \left( \cos \frac{(2k+1)\pi}{n} + \sqrt{-1} \sin \frac{(2k+1)\pi}{n} \right),$$

où $\rho$ désigne $1 + x$ ou $-(1 + x)$ et où $\rho^{\frac{m}{n}}$ n'a qu'une valeur positive.

La théorie indique que, quelle que soit la position du point de départ $[x_0, y_0]$, la région de convergence ne pourra jamais couper qu'une seule des branches de la conjuguée dangereuse; d'un autre côté, tous les points correspondants à une même abscisse seront toujours séparés les uns des autres par une au moins de ces branches; par conséquent, si l'on savait quelle est la branche que peut couper la limite de la région de convergence, on saurait par là même dans quelle case se trouvera le point d'arrivée : il appartiendrait à la case qui contenait le point de départ, ou à la case voisine, entamée par la région de convergence, suivant que $\beta_0$ et $\beta_1$ seraient de même signe ou de signes contraires.

Or, en supposant à $x_0$ une valeur réelle 0, et se donnant en outre la valeur initiale de $y$, on se donne par là même la branche de la conjuguée $C = \infty$ qui traverse la région de convergence : la question est donc résolue d'avance, il ne reste qu'à en donner la réponse en formule.

Pour cela posons

$$1 + x = \rho(\cos\varphi + \sqrt{-1}\sin\varphi),$$

$\varphi$ devant partir de o en même temps que $x$; il en résultera

$$y = \rho^{\frac{m}{n}}\left(\cos\frac{2k\pi + m\varphi}{n} + \sqrt{-1}\sin\frac{2k\pi + m\varphi}{n}\right).$$

S'il ne s'agissait pas de retrouver dans cette formule la valeur de $y$ qui se développe par la série de Maclaurin, on pourrait y donner à $\varphi$ et à $\rho$ toutes les valeurs imaginables.

Mais en premier lieu, pour que la série soit convergente, il faudra que $\rho$ reste compris entre o et 2, et d'un autre côté, la discussion précédente prouve qu'en raison de cette condition la valeur de la série reproduira bien de temps à autre la valeur de

$$\rho^{\frac{m}{n}}\left(\cos\frac{2k\pi}{n} + \sqrt{-1}\sin\frac{2k\pi}{n}\right),$$

dans laquelle $k$ correspondrait à $y_0$ mais ne se rencontrera jamais même avec les valeurs voisines algébriquement

$$\rho^{\frac{m}{n}}\left(\cos\frac{(2k\pm 1)\pi}{n} + \sqrt{-1}\sin\frac{(2k\pm 1)\pi}{n}\right):$$

cela signifie évidemment que, pour que la formule

$$\rho^{\frac{m}{n}}\left(\cos\frac{2k\pi + m\varphi}{n} + \sqrt{-1}\sin\frac{2k\pi + m\varphi}{n}\right)$$

reproduise perpétuellement la valeur de la série, il faudra que $m\varphi$ reste toujours compris entre $+\pi$ et $-\pi$, c'est-à-dire que si $x = \alpha + \beta\sqrt{-1}$ est la valeur finale qu'on veut attribuer à $x$ et qui devra être telle, que $\alpha^2 + \beta^2 < 1$, pour mettre d'accord les deux formules, il faudra toujours, après avoir tiré $\varphi$ des équations

$$\sin\varphi = \frac{\beta}{\sqrt{(1+\alpha)^2 + \beta^2}}, \quad \cos\varphi = \frac{1+\alpha}{\sqrt{(1+\alpha)^2+\beta^2}},$$

réduire $m\varphi$, par l'addition ou la soustraction d'un nombre convenable de circonférences, à rentrer dans les limites

$$-\pi < m\varphi < +\pi.$$

**115.** L'équation

$$y = \mathrm{L}(1 + x)$$

donne lieu à une discussion analogue : le point dangereux a encore pour abscisse $x = 0$, de sorte que la conjuguée dangereuse est toujours la conjuguée $C = \infty$ dont les branches sont représentées, du côté des $x$ plus grands que $-1$ par les équations

$$y = \mathrm{L}(1 + x) + 2k\pi\sqrt{-1},$$

et du côté des $x$ moindres que $-1$ par

$$y = \mathrm{L}(-1 - x) + (2k + 1)\pi\sqrt{-1}.$$

Quel que soit le point de départ $[x_0, y_0]$, la région de convergence ne pourra jamais couper qu'une seule branche de la conjuguée dangereuse; d'un autre côté, si $x_0 = 0$ et $y_0 = 2k_0\pi\sqrt{-1}$, c'est la branche

$$y = \mathrm{L}(1 + x) + 2k_0\pi\sqrt{-1}$$

qui traversera la région de convergence : on sait donc d'avance que le point $[x_1, y_1]$ dont l'ordonnée serait fournie par la série de Maclaurin, supposée convergente, sera compris entre les branches

$$y = \mathrm{L}(1 + x) + 2k_0\pi\sqrt{-1}$$

d'une part, et

$$y = \mathrm{L}(1 + x) + (2k_0 \pm 2)\pi\sqrt{-1}$$

de l'autre. Ce qui fournit la solution géométrique de la question.

Pour en avoir la solution algébrique, posons

$$1 + x = \rho(\cos\varphi + \sqrt{-1}\sin\varphi),$$

d'où

$$y = \mathrm{L}.\rho + \varphi\sqrt{-1}.$$

il est clair que, pour que cette formule reste constamment d'accord avec la série, il faudra que $\varphi$ lui-même reste compris entre

$$(2k_0+1)\pi \quad \text{et} \quad (2k_0-1)\pi,$$

puisque sans cela, $\varphi$, variant d'une manière continue de sa valeur initiale $2k_0\pi$ à sa valeur finale, aurait pris momentanément l'une des valeurs

$$(2k_0 \pm 1)\pi,$$

ce qui eût amené le point $[x, y]$ sur l'une des branches

$$y = \mathrm{L}(-1-x) + (2k_0 \pm 1)\pi\sqrt{-1}$$

que la région de convergence ne peut pas atteindre.

Le même procédé de démonstration s'étendrait sans peine aux fonctions

$$y = \int dx \sqrt{\frac{1-x^2}{1-e^2x^2}},$$

$$y = \int dx \frac{1}{\sqrt{(1-x^2)(1-e^2x^2)}},$$

et en général à toutes les intégrales périodiques.

**114.** Dans les exemples précédents, la région de convergence de la série était toujours limitée à celui des points dangereux dont l'abscisse, retranchée de celle du point de départ, fournissait la différence de plus petit module : il n'en sera plus de même dans les exemples qui vont suivre et qui par suite présenteront un intérêt nouveau.

Soit d'abord l'équation

$$y^3 - a^2y + a^2x = 0,$$

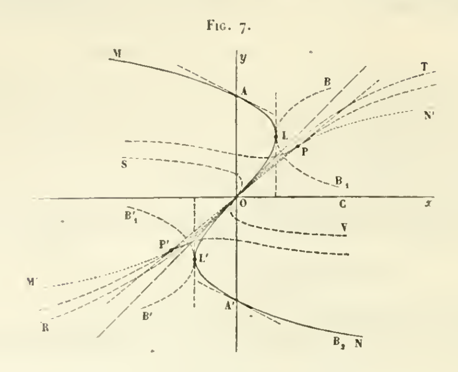
que nous avons déjà étudiée dans le chapitre VI.

Les points dangereux sont (*fig.* 7)

$$\mathrm{L}\begin{cases} x = \dfrac{2a}{3\sqrt{3}} \\ y = \dfrac{a}{\sqrt{3}} \end{cases} \quad \text{et} \quad \mathrm{L}'\begin{cases} x = -\dfrac{2a}{3\sqrt{3}}, \\ y = -\dfrac{a}{\sqrt{3}}. \end{cases}$$

les carrés des modules des différences des abscisses des deux points

Fig. 7.



dangereux retranchées successivement de celle d'un point quelconque du lieu,

$$\begin{cases} x = \alpha + \beta\sqrt{-1}, \\ y = \alpha' + \beta'\sqrt{-1}, \end{cases}$$

sont

$$\left(\alpha - \frac{2a}{3\sqrt{3}}\right)^2 + \beta^2 \quad \text{et} \quad \left(\alpha + \frac{2a}{3\sqrt{3}}\right)^2 + \beta^2$$

dont l'égalité n'exige que l'annulation de $\alpha$.

Il semblerait donc que la région de convergence de la série dût passer à la fois aux deux points dangereux dès que l'abscisse du point de départ serait dépourvue de partie réelle ; et que, par les mêmes motifs, la région de convergence fût limitée au point L si $\alpha_0$ était positif et au point L' dans le cas contraire.

Mais ces conclusions sont le plus souvent démenties par les faits, car pour aller du point de départ à celui des deux points dangereux dont la distance modulaire serait la plus petite, il faut quelquefois ou passer d'abord par l'autre point dangereux, ou aller prendre passage, plus loin encore, sur la branche de conjuguée qui contient cet autre point.

C'est qu'en effet la formule que l'on possède de la condition de con-

vergence, ne contenant que les parties réelles et imaginaires de la variable indépendante, à ses deux limites, tandis qu'elle devrait au moins contenir les parties qui composent la valeur initiale de la fonction, il serait imprudent de s'abandonner complétement aux indications qu'elle peut fournir; il faut l'appliquer seulement de proche en proche, avec précautions, et encore doit-on rejeter les conclusions où elle mènerait lorsque ces conclusions sont en contradiction évidente avec les faits.

Dans l'exemple qui nous occupe, $\alpha$ peut s'annuler dans des circonstances toutes différentes et où les conclusions à tirer ne sont en rien semblables.

$\alpha$ s'annule d'abord lorsque le point $[x,y]$ passe sur l'enveloppe imaginaire : dans ce cas on conçoit aisément que la région de convergence s'étende également jusqu'aux deux points dangereux; car, en vertu de l'inégalité

$$\beta_0^2 < \frac{4a^3}{27} + \beta_0^2,$$

elle comprendra nécessairement l'origine : or si le point $[x,y]$ peut se rendre du point de départ $[\beta_0, \beta'_0]$ à l'origine, il aura ensuite le même chemin à faire pour aller soit à l'un, soit à l'autre des deux points dangereux.

Mais chacune des conjuguées dont la caractéristique surpasse $-\frac{1}{2}$ contient aussi deux points dont les abscisses manquent de partie réelle. Ces conjuguées touchent la courbe réelle sur les arcs AM et A'N; or il sera facile d'établir, ce qui d'ailleurs est pour ainsi dire évident, que si le point de départ appartient, par exemple, à une branche tangente à la courbe réelle en un point de l'arc AM, soit que la partie réelle de l'abscisse de ce point de départ soit d'ailleurs positive, nulle, ou négative, ce sera toujours le point L qui limitera la région de convergence, tandis que le point L' en sera séparé par un intervalle plus ou moins considérable.

Nous remarquerons encore, avant d'entrer dans les détails, que si le point de départ appartient à une conjuguée tangente à l'enveloppe imaginaire, la partie imaginaire de son abscisse sera positive ou néga-

tive selon que le point de contact, avec l'enveloppe, de la demi-conjuguée où se trouvera ce point de départ, appartiendra à la branche ON′ ou à la branche OM′; et que si ce contact a lieu, par exemple, sur ON′, la partie réelle de l'abscisse du point de départ sera positive ou négative, selon que la branche qui contiendra le point de départ s'éloignera du point de contact vers la droite ou vers la gauche.

Cela posé, prenons d'abord pour point de départ un point d'une demi-conjuguée tangente à la courbe réelle en un point de l'arc LM : pour parvenir au point L′, il faudrait que le point $[x, y]$ passât d'abord sur la demi-conjuguée qui touche la courbe réelle en L : mais si l'on compare les carrés des modules des différences des abscisses du point L et d'un point de la conjuguée qui y passe, retranchées successivement de l'abscisse du point de départ, on voit que de ces deux carrés

$$\left(\alpha_0 - \frac{2a}{3\sqrt{3}}\right)^2 + \beta_0^2,$$

$$\left(\alpha_0 - \frac{2a}{3\sqrt{3}} - h\right)^2 + \beta_0^2,$$

le premier est inférieur au second, dès que $\alpha_0$ n'atteint pas $\frac{2a}{3\sqrt{3}}$, puisque $h$ est supposé positif.

Ainsi, il ne serait pas même nécessaire que $\alpha_0$ fût négatif; il suffirait qu'il fût moindre que $\frac{2a}{3\sqrt{3}}$ pour que le point $[x, y]$, bien loin de pouvoir atteindre au point L′, ne pût même pas passer sur la conjuguée qui touche la courbe réelle au point dangereux L.

Tant donc que la demi-conjuguée passant par le point de départ touchera la courbe réelle en un point de l'arc LM, la région de convergence sera limitée au point L : si $\alpha_0$ est moindre que $\frac{2a}{3\sqrt{3}}$, le point $[x, y]$ ne pourra pas passer sur la conjuguée qui touche la courbe réelle en L, tandis que si $\alpha_0$ surpasse $\frac{2a}{3\sqrt{3}}$, le point $[x, y]$ au contraire ne pourra pas passer sur la courbe réelle.

Dans le premier cas, le point d'arrivée appartiendra encore à une demi-conjuguée tangente à la courbe réelle en un point de l'arc LM;

et les deux points de départ et d'arrivée seront sur leurs conjuguées respectives placés, par rapport aux points de contacts de ces conjuguées avec la courbe réelle, du même côté, ou de côtés opposés, suivant que $\beta_1 \beta_0$ sera positif ou négatif, parce que si $\beta$ a passé par zéro dans l'intervalle, à ce moment le point $[x, y]$ aura changé de branche sur la conjuguée qui le contenait.

Dans le second cas, où $\alpha_0$ surpasserait $\frac{2a}{3\sqrt{3}}$, le point $[x, y]$ ne pourra pas atteindre la courbe réelle, mais il pourra traverser la demi-conjuguée qui passe au point L, sur sa branche supérieure ou sa branche inférieure, suivant que $\beta_0$ sera positif ou négatif; et il l'aura traversée en effet si $\beta_1 \beta_0$ est négatif, tandis que si au contraire $\beta_1 \beta_0$ est positif, le point de contact, avec la courbe réelle de la branche de conjuguée à laquelle appartiendra le point d'arrivée, sera resté sur l'arc ML.

Lorsque le point $[x, y]$ aura traversé la conjuguée $C = \infty$, le point de contact avec la courbe réelle de la branche de conjuguée à laquelle appartiendra le point d'arrivée, sera sur l'arc LO, ou bien cette branche de conjuguée ne touchera plus la courbe réelle.

Dans cette dernière hypothèse, le point $[x, y]$ aurait traversé la conjuguée $C = 1$, en un point de la branche TOV, sur l'arc OT, si $\beta_0$ était positif, et sur OV dans le cas contraire.

La conjuguée $C = 1$ est fournie par les équations

$$\alpha'^3 - 3\alpha'\beta^2 - a^2\alpha' + a^2\alpha = 0$$

et

$$3\alpha'^2 = \beta^2,$$

d'où l'on tire

$$\alpha = \pm\left(\frac{8\beta^3}{3a^2\sqrt{3}} + \frac{\beta}{\sqrt{3}}\right),$$

le signe + convenant à l'arc ROT et le signe — à SOV, car sur OT, $\alpha$ et $\beta$ sont positifs, sur OV, $\alpha$ est positif et $\beta$ négatif, sur OS, $\alpha$ est négatif et $\beta$ positif, enfin sur OR, $\alpha$ et $\beta$ sont négatifs.

Comme aucune des conjuguées circonscrites à l'enveloppe imaginaire, excepté la conjuguée $C = 1$, ne coupe l'axe des $x$, car les équa-

tions

$$\begin{aligned} \alpha'^3 - 3\alpha'\beta^2 C^2 - \alpha^2\alpha' + a^2\alpha = 0, \\ 3\alpha'^2\beta C - \beta^3 C^3 - a^2\beta C + a^2\beta = 0, \\ \alpha' + \beta C = 0, \end{aligned}$$

donnent

$$\beta = \pm a\sqrt{\frac{C-1}{2C^3}}.$$

Il en résulte que les deux arcs OS et OT sont les limites respectives des branches de gauche et de droite d'une conjuguée tangente à l'enveloppe imaginaire en un point situé sur ON', à une distance infiniment petite du point O; et que de même OV et OR sont les limites des branches de droite et de gauche d'une conjuguée tangente à l'enveloppe imaginaire en un point situé sur OM' à une distance infiniment petite du point O.

On conclut de là et de ce que, dans l'hypothèse où nous raisonnons, $\alpha_0 > \frac{2a}{3\sqrt{3}}$, le point $[x, y]$ ne pouvant passer sur la courbe réelle, ne peut non plus changer de branche sur la conjuguée où il se trouve : que si le point de départ appartient à une branche supérieure le point mobile ne pourra traverser la conjuguée $C = 1$ qu'en un point de OT, ce qu'on reconnaîtra à l'inégalité

$$\left(\alpha_0 - \frac{8\beta_0^3}{3a^2\sqrt{3}} - \frac{\beta_0}{\sqrt{3}}\right)\left(\alpha_1 - \frac{8\beta_1^3}{3a^2\sqrt{3}} - \frac{\beta_1}{\sqrt{3}}\right) < 0,$$

auquel cas le point d'arrivée appartiendra à une conjuguée tangente à l'enveloppe imaginaire en un point de ON'; et qu'au contraire, si le point de départ appartient à une branche inférieure, le point $[x, y]$ ne pourra traverser la conjuguée $C = 1$ qu'en un point de OV, ce qu'on reconnaîtra à l'inégalité

$$\left(\alpha_0 + \frac{8\beta_0^3}{3a^2\sqrt{3}} + \frac{\beta_0}{\sqrt{3}}\right)\left(\alpha_1 + \frac{8\beta_1^3}{3a^2\sqrt{3}} + \frac{\beta_1}{\sqrt{3}}\right) < 0,$$

auquel cas le point d'arrivée appartiendra à une branche de conjuguée tangente à l'enveloppe imaginaire en un point de OM'.

Au reste la condition de convergence

$$(\alpha-\alpha_0)^2+(\beta-\beta_0)^2<\left(\alpha_0-\frac{2a}{3\sqrt{3}}\right)^2+\beta_0^2$$

se réduisant à

$$\alpha_0^2+(\beta-\beta_0)^2<\left(\alpha_0-\frac{2a}{3\sqrt{3}}\right)^2+\beta_0^2,$$

pour un point de l'enveloppe imaginaire, cette inégalité ne pourra pas être satisfaite, dans le cas où nous sommes, puisque $\alpha_0$ étant plus grand que $\frac{2a}{3\sqrt{3}}$, $\alpha_0^2$ sera déjà plus grand que $\left(\alpha_0-\frac{2a}{3\sqrt{3}}\right)^2$ et que d'un autre côté le point $[x, y]$ ayant traversé la conjuguée $C=\infty$, $\beta$ et $\beta_0$ seraient de signes contraires, ce qui rendrait $(\beta-\beta_0)^2$ plus grand aussi que $\beta_0^2$.

Ainsi tant que le point de départ appartiendra à une branche de conjuguée tangente à la courbe réelle en un point de ML, le point $[x, y]$ ne pourra pas atteindre l'enveloppe imaginaire des conjuguées.

Supposons maintenant que le point de départ appartienne à une branche de conjuguée tangente à la courbe réelle en un point de l'arc LO.

La condition de convergence

$$(\alpha-\alpha_0)^2+(\beta-\beta_0)^2<\left(\alpha_0-\frac{2a}{3\sqrt{3}}\right)^2+\beta_0^2$$

se réduisant à

$$\left(\alpha-\frac{2a}{3\sqrt{3}}\right)\left(\alpha+\frac{2a}{3\sqrt{3}}-2\alpha_0\right)<0$$

lorsqu'on y fait $\beta=0$, on voit que le point $[x, y]$ pourra passer sur la conjuguée $C=\infty$, qui a son contact en L, sans pouvoir atteindre la courbe réelle, ou inversement, suivant que $\alpha_0$ sera plus grand ou plus petit que $\frac{2a}{3\sqrt{3}}$.

Dans le cas où $\alpha_0$ serait plus grand que $\frac{2a}{3\sqrt{3}}$, le point $[x, y]$ aurait retraversé la conjuguée $C=\infty$ si $\beta_1\beta_0$ avait le signe $-$; mais ce cas n'offre plus aucun intérêt.

Que $\alpha_0$ soit plus grand ou plus petit que $\frac{2a}{3\sqrt{3}}$, le point $[x, y]$ pourra occasionnellement traverser la conjuguée $C = 1$, et il l'aura traversée en effet si

$$\left[\alpha_0^2 - \left(\frac{8\beta_0^3}{3a^2\sqrt{3}} + \frac{\beta_0}{\sqrt{3}}\right)^2\right]\left[\alpha_1^2 - \left(\frac{8\beta_1^3}{3a^2\sqrt{3}} + \frac{\beta_1}{\sqrt{3}}\right)^2\right]$$

est négatif.

Il pourra même atteindre l'enveloppe imaginaire des conjuguées si la distance modulaire

$$\sqrt{\left(\alpha_0 - \frac{2a}{3\sqrt{3}}\right)^2 + \beta_0^2}$$

est assez considérable.

Car $\beta$ et $\beta_0$ devant être maintenant de même signe, l'inégalité

$$\alpha_0^2 + (\beta - \beta_0)^2 < \left(\alpha_0 - \frac{2a}{3\sqrt{3}}\right)^2 + \beta_0^2$$

ou

$$\beta^2 - 2\beta\beta_0 + \frac{4a\alpha_0}{3\sqrt{3}} - \frac{4a^2}{27} < 0$$

ne présenterait d'impossibilité qu'autant que

$$\beta_0^2 - \frac{4a\alpha_0}{3\sqrt{3}} + \frac{4a^2}{27}$$

serait négatif; c'est-à-dire que

$$\beta_0^2 + \left(\alpha_0 - \frac{2a}{3\sqrt{3}}\right)^2 < \alpha_0^2,$$

de sorte que

$$\beta_0^2 + \left(\alpha_0 - \frac{2a}{3\sqrt{3}}\right)^2 - \alpha_0^2 = 0$$

serait l'équation du lieu qui séparerait les points pour lesquels la région de convergence n'atteindrait pas l'enveloppe imaginaire, de ceux au contraire d'où la série pourrait rayonner au delà de cette enveloppe.

Au reste l'enveloppe imaginaire des conjuguées étant caractérisée par la condition

$$\alpha = 0,$$

le signe de $\alpha_0\,\alpha_1$ indiquera toujours si le point $[x, y]$ a ou non passé sur cette enveloppe.

Supposons donc $\alpha_0 < \frac{2a}{3\sqrt{3}}$, pour que le point $[x, y]$ puisse passer sur la courbe réelle.

Ce cas se subdivisera en deux autres suivant que $\alpha_0$ sera plus grand ou plus petit que $\frac{a}{3\sqrt{3}}$. Dans la première hypothèse, en effet, le chemin du point $[x, y]$ ne pourra rencontrer la courbe réelle qu'en un point de l'arc OL, tandis que dans le cas contraire il pourrait la rencontrer sur l'arc OL'.

En effet, la condition de convergence, pour un point de la courbe réelle, se réduisant à

$$(\alpha - \alpha_0)^2 + \beta_0^2 < \left(\alpha_0 - \frac{2a}{3\sqrt{3}}\right)^2 + \beta_0^2$$

ou

$$\left(\alpha - \frac{2a}{3\sqrt{3}}\right)\left(\alpha + \frac{2a}{3\sqrt{3}} - 2\alpha_0\right) < 0,$$

elle ne pourra être satisfaite par une valeur négative de $\alpha$ qu'autant que $\alpha_0$ sera moindre que $\frac{a}{3\sqrt{3}}$.

Supposons d'abord $\alpha_0 > \frac{a}{3\sqrt{3}}$. Dans ce cas si le point $[x, y]$ passe sur la courbe réelle, ce qu'on reconnaîtra au caractère

$$\beta_0\beta_1 < 0,$$

il reviendra sur des conjuguées tangentes à la branche OL, si

$$\left[\alpha_0^2 - \left(\frac{8\beta_0^3}{3a^2\sqrt{3}} + \frac{\beta_0}{\sqrt{3}}\right)^2\right]\left[\alpha_1^2 - \left(\frac{8\beta_1^3}{3a^2\sqrt{3}} + \frac{\beta_1}{\sqrt{3}}\right)^2\right] > 0 :$$

dans le cas contraire il aura traversé la conjuguée $C = 1$ et se sera transporté sur une conjuguée tangente à l'enveloppe imaginaire.

Si au contraire $\alpha_0$ est moindre que $\frac{a}{3\sqrt{3}}$, le point $[x, y]$ avant d'arriver à la branche OL', aura dû passer sur l'enveloppe imaginaire des conjuguées pour que $\alpha$ ait pu changer de signe. De sorte que si $\alpha_1 \alpha_0$ avait le signe $+$, le point $[x, y]$ n'aurait pas passé sur la branche OL'.

On pourrait maintenant placer le point de départ sur une conjuguée tangente à l'enveloppe imaginaire en un point de l'arc ON'.

Mais il serait inutile de reprendre en détail l'analyse des faits dans cette hypothèse : nous venons de passer des conjuguées d'une catégorie à celles de l'autre, on effectuerait aussi aisément le passage inverse.

**115.** Nous étudierons en dernier lieu l'équation

$$y^3 - 3axy + x^3 = 0,$$

dont l'exemple, par les difficultés qu'il semblerait devoir présenter, fournira un contrôle suffisant de la méthode.

L'origine est un point double où les deux tangentes sont distinctes; mais comme l'une d'elles se confond avec l'axe des $y$, ce point pourra dans certains cas borner la région de convergence.

La dérivée de $y$, par rapport à $x$, redevient infinie aux points

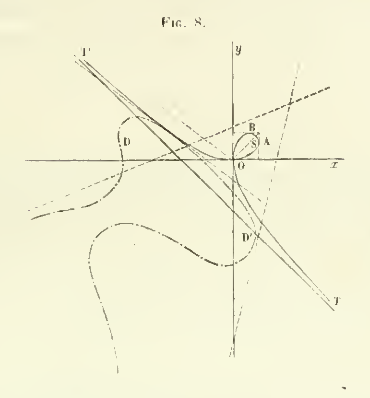
$$\begin{cases} x = a\sqrt[3]{4}, \\ y = a\sqrt[3]{2}, \end{cases}$$

$$\begin{cases} x = a\sqrt[3]{4}\,\dfrac{-1-\sqrt{3}\sqrt{-1}}{2}, \\ y = a\sqrt[3]{2}\,\dfrac{-1+\sqrt{3}\sqrt{-1}}{2}, \end{cases}$$

$$\begin{cases} x = a\sqrt[3]{4}\,\dfrac{-1+\sqrt{3}\sqrt{-1}}{2}, \\ y = a\sqrt[3]{2}\,\dfrac{-1-\sqrt{3}\sqrt{-1}}{2}. \end{cases}$$

Ces trois points A, D, D′ (*fig* 8) sont encore des points dangereux.

Fig. 8.




Toutes les conjuguées touchent la courbe réelle; leur enveloppe imaginaire ne jouera dans la discussion qu'un rôle très-secondaire.

La courbe a pour asymptotes les droites

$$y = -x - a,$$

$$y = \frac{1-\sqrt{3}\sqrt{-1}}{2}x + \frac{2a}{1-\sqrt{3}\sqrt{-1}},$$

$$y = \frac{1+\sqrt{3}\sqrt{-1}}{2}x + \frac{2a}{1+\sqrt{3}\sqrt{-1}}.$$

La caractéristique commune des points dangereux imaginaires est $-\frac{1}{\sqrt[3]{2}}$, celle des points dangereux réels est infinie.

Outre la courbe réelle, la figure représente la partie de la conjuguée $C = -\frac{1}{\sqrt[3]{2}}$ qui contient les points dangereux imaginaires; cette conjuguée a été construite avec soin par M. J. Fontès, candidat à l'École Polytechnique.

Supposons d'abord le point de départ situé sur une branche de conjuguée tangente à l'arc OT de la courbe réelle; la région de con-

vergence sera alors limitée au point O : en effet, si $\alpha_0$ est positif, le point $[x, y]$ ne pourra même pas atteindre la portion de la conjuguée $C = \infty$ qui touche la courbe réelle à l'origine, car l'inégalité

$$(\alpha - \alpha_0)^2 + \beta_0^2 < \alpha_0^2 + \beta_0^2,$$

ne pouvant être satisfaite par aucune valeur négative de $\alpha$, si le point $[x, y]$ pouvait se rendre sur la portion de la conjuguée $C = \infty$ dont nous parlons, il pourrait à plus forte raison passer à l'origine en suivant un chemin tangent à l'axe des $y$, ce qui n'est possible en aucun cas.

D'un autre côté si $\alpha_0$ est négatif, l'inégalité

$$\alpha_0^2 + \beta_0^2 < (\alpha_0 - a\sqrt[3]{4})^2 + \beta_0^2$$

suffit pour montrer que le point A sera certainement au dehors de la région de convergence, que par conséquent le point $[x, y]$ ne pourra atteindre la portion de la conjuguée $C = \infty$ qui touche la courbe réelle en A, et que, à plus forte raison, il restera bien éloigné de la branche de la conjuguée $C = -\frac{1}{\sqrt[3]{2}}$ qui contient les points dangereux imaginaires.

Cela posé, si $\alpha_0$ est positif, le point $[x, y]$ pourra passer sur la courbe réelle et il y aura passé en effet, si $\beta_1\beta_0$ est négatif; mais la caractéristique du point final sera restée en tout cas négative et moindre que $-1$.

Au contraire si $\alpha_0$ est négatif, le point $[x, y]$ pourra passer sur la portion de la conjuguée $C = \infty$ qui touche la courbe réelle à l'origine; il y aura passé en effet si $\beta_1\beta_0$ est négatif, et dans ce cas la caractéristique du point d'arrivée sera devenue positive; tandis que, si $\beta_1\beta_0$ est positif, cette caractéristique sera restée négative et moindre que $-1$.

Plaçons maintenant le point de départ sur une branche de conjuguée tangente à la courbe réelle en un point de l'arc OBSA.

La région de convergence restera limitée à l'origine tant que $\alpha_0^2 + \beta_0^2$ sera moindre que $(\alpha_0 - a\sqrt[3]{4})^2 + \beta_0^2$, c'est-à-dire tant que $\alpha_0$ ne sur-

passera pas $\frac{a}{\sqrt[3]{2}}$, ce qui ne saurait évidemment arriver sur une conjuguée très-voisine de celle qui passe par l'origine avec une caractéristique infinie.

Ainsi le point de départ marchant toujours dans le même sens, la région de convergence restera d'abord, et pendant un certain temps, limitée à l'origine.

On pourrait évidemment préciser davantage, si on le voulait.

Le point de départ étant choisi de manière que la région de convergence reste limitée à l'origine : si $\alpha_0$ est négatif, le point $[x, y]$ pourra passer sur la branche de la conjuguée $C = \infty$ qui touche la courbe réelle à l'origine, mais il ne pourra atteindre la courbe réelle; dans le cas contraire il pourra passer sur la courbe réelle, mais non sur la conjuguée $C = \infty$.

D'un autre côté la conjuguée $C = 0$, qui touche la courbe réelle au point B, étant définie par les équations

$$y^3 - 3a\alpha y + \alpha^3 - 3\alpha\beta^2 = 0, \quad -3ay + 3\alpha^2 - \beta^2 = 0.$$

d'où l'on tire par l'élimination de $y$

$$\left(\frac{3\alpha^2 - \beta^2}{3a}\right)^3 - 2\alpha(\alpha^2 + \beta^2) = 0,$$

suivant que

$$\left[\left(\frac{3\alpha_0^2 - \beta_0^2}{3a}\right)^3 - 2\alpha_0(\alpha_0^2 + \beta_0^2)\right]\left[\left(\frac{3\alpha_1^2 - \beta_1^2}{3a}\right)^3 - 2\alpha_1(\alpha_1^2 + \beta_1^2)\right]$$

sera positif ou négatif, le point $[x, y]$ n'aura pas, ou aura passé sur cette conjuguée $C = 0$.

Cela posé, on peut distinguer les deux cas où le point de départ se trouverait entre les deux portions des conjuguées $C = \infty$, $C = 0$, qui nous occupent, ou au delà de la conjuguée $C = 0$.

Dans le premier cas, et si d'ailleurs $\alpha_0$ est négatif, suivant que $\beta_1\beta_0$ aura le signe $-$ ou le signe $+$, le point d'arrivée appartiendra à une portion de conjuguée tangente à la courbe réelle, en un point de l'arc ASBOT, situé au-dessous ou au-dessus de l'origine. Si donc $\beta_1\beta_0$ a le signe $-$, le point $[x, y]$ n'aura pas passé sur la conjuguée $C = 0$, ou

y aura passé un nombre pair de fois, ce qui revient au même, et la caractéristique du point d'arrivée sera négative; mais si $\beta_1\beta_0$ a le signe $+$, le point $[x, y]$ n'aura pas traversé la conjuguée $C = \infty$, ou l'aura traversée un nombre pair de fois, ce qui revient au même, et la caractéristique du point d'arrivée sera positive ou négative suivant que

$$\left[\left(\frac{3\alpha_0^2 - \beta_0^2}{3a}\right)^3 - 2\alpha_0(\alpha_0^2 + \beta_0^2)\right]\left[\left(\frac{3\alpha_1^2 - \beta_1^2}{3a}\right)^3 - 2\alpha_1(\alpha_1^2 + \beta_1^2)\right]$$

sera positif ou négatif.

Si au contraire $\alpha_0$ était positif, le point $[x, y]$ ne pouvant plus passer sur la conjuguée $C = \infty$, la caractéristique du point d'arrivée serait positive ou négative suivant que

$$\left[\left(\frac{3\alpha_0^2 - \beta_0^2}{3a}\right)^3 - 2\alpha_0(\alpha_0^2 + \beta_0^2)\right]\left[\left(\frac{3\alpha_1^2 - \beta_1^2}{3a}\right)^3 - 2\alpha_1(\alpha_1^2 + \beta_1^2)\right]$$

serait positif ou négatif; et comme d'ailleurs le point $(x, y)$ aura ou non passé sur la courbe réelle, suivant que $\beta_1\beta_0$ aura le signe $-$ ou le signe $+$ : si $\beta_1\beta_0$ est négatif, le point d'arrivée sera sur une branche de conjuguée dirigée à droite ou à gauche, si le point de départ appartenait à une branche dirigée à gauche ou à droite, et inversement, si $\beta_1\beta_0$ a le signe $+$.

Dans le second cas, où le point de départ se trouverait au delà de la conjuguée $C = 0$, si $\alpha_0$ est négatif, la caractéristique du point d'arrivée sera négative ou positive suivant que

$$\beta_1\beta_0\left[\left(\frac{3\alpha_0^2 - \beta_0^2}{3a}\right)^3 - 2\alpha_0(\alpha_0^2 + \beta_0^2)\right]\left[\left(\frac{3\alpha_1^2 - \beta_1^2}{3a}\right)^3 - 2\alpha_1(\alpha_1^2 + \beta_1^2)\right]$$

sera positif ou négatif, car il n'aura traversé ni la conjuguée $C = 0$ ni à plus forte raison la conjuguée $C = \infty$, si

$$\left[\left(\frac{3\alpha_0^2 - \beta_0^2}{3a}\right)^3 - 2\alpha_0(\alpha_0^2 + \beta_0^2)\right]\left[\left(\frac{3\alpha_1^2 - \beta_1^2}{3a}\right)^3 - 2\alpha_1(\alpha_1^2 + \beta_1^2)\right]$$

a le signe $+$; il aura seulement traversé la conjuguée $C = 0$, si

$$\left[\left(\frac{3\alpha_0^2 - \beta_0^2}{3a}\right)^3 - 2\alpha_0(\alpha_0^2 - \beta_0^2)\right]\left[\left(\frac{3\alpha_1^2 - \beta_1^2}{3a}\right)^3 - 2\alpha_1(\alpha_1^2 + \beta_1^2)\right]$$

a le signe $-$, $\beta_1\beta_0$ ayant au contraire le signe $+$ ; enfin il aura traversé les deux conjuguées si les deux produits ont chacun le signe $-$.

Si $\alpha_0$ est au contraire positif, le point $[x, y]$ ne pouvant passer sur la conjuguée $C=\infty$, la caractéristique du point d'arrivée sera négative ou positive suivant que

$$\left[\left(\frac{3\alpha_0^2-\beta_0^2}{3a}\right)^3 - 2\alpha_0(\alpha_0^2+\beta_0^2)\right]\left[\left(\frac{3\alpha_1^2-\beta_1^2}{3a}\right)^3 - 2\alpha_1(\alpha_1^2+\beta_1^2)\right]$$

sera positif ou négatif : d'ailleurs si $\beta_1\beta_0$ est négatif, le point d'arrivée appartiendra à une branche dirigée vers la droite ou vers la gauche, si le point de départ se trouvait sur une branche dirigée à gauche ou à droite, et inversement si $\beta_1\beta_0$ a le signe $+$.

Supposons maintenant le point de départ placé toujours sur une branche de conjuguée tangente à la courbe réelle en un point de l'arc OBSA, mais avec la circonstance

$$\alpha_0 > \frac{a}{\sqrt[3]{2}}.$$

Le point $[x, y]$ ne pourra passer sur la portion de la conjuguée $C=\infty$ qui touche la courbe réelle en A que si l'on peut satisfaire à l'inégalité

$$(\alpha-\alpha_0)^2+\beta_0^2 < (\alpha_0 - a\sqrt[3]{4})^2+\beta_0^2$$

par des valeurs de $\alpha$ dépassant $+a\sqrt[3]{4}$ : or cette inégalité se réduit à

$$\alpha^2 - 2\alpha_0\alpha + 2a\alpha_0\sqrt[3]{4} - 2a^2\sqrt[3]{2} < 0,$$

et exige que $\alpha$ reste compris entre

$$2\alpha_0 - a\sqrt[3]{4} \quad \text{et} \quad a\sqrt[3]{4}:$$

comme nous supposons $\alpha_0 > \frac{a}{\sqrt[3]{2}}$, $2\alpha_0 - a\sqrt[3]{4}$ sera positif. Mais il reste cependant à distinguer deux cas :

$$2\alpha_0 - a\sqrt[3]{4} < a\sqrt[3]{4} \quad \text{et} \quad 2\alpha_0 - a\sqrt[3]{4} > a\sqrt[3]{4},$$

c'est-à-dire

$$\alpha_0 < a\sqrt[3]{4} \quad \text{et} \quad \alpha_0 > a\sqrt[3]{4};$$

dans le premier en effet, pour satisfaire à l'inégalité

$$(\alpha - \alpha_0)^2 + \beta_0^2 < (\alpha_0 - a\sqrt[3]{4})^2 + \beta_0^2,$$

il faudrait que $\alpha$ restât moindre que $a\sqrt[3]{4}$, ce qui veut dire que le point $[x, y]$ ne pourrait pas atteindre la portion de la conjuguée $C = \infty$ qui touche la courbe réelle en A; tandis que dans le second cas, pour satisfaire à la même inégalité, il faudrait que $\alpha$ restât plus grand que $a\sqrt[3]{4}$, ce qui signifie que le point $[x, y]$ ne pourrait plus revenir à la courbe réelle.

Supposons $\alpha_0 < a\sqrt[3]{4}$, le point $[x, y]$ ne pouvant dans ce cas passer sur la portion de la conjuguée $C = \infty$ qui touche la courbe réelle en A, ne pourra, à plus forte raison, atteindre la conjuguée $C = -\frac{1}{\sqrt[3]{2}}$; par conséquent, la région de convergence sera bien limitée au point A.

Quelque part qu'on plaçât le point de départ, on saurait, dans cette hypothese, comme précédemment, quel serait le signe de la caractéristique du point d'arrivée, et sur quelle branche ce point se trouverait.

Je passe donc au cas où $\alpha_0$ dépasserait $a\sqrt[3]{4}$. Le point $[x, y]$ pouvant alors traverser la portion de la conjuguée $C = \infty$ qui touche la courbe réelle au point A, on ne voit pas tout d'abord pourquoi il ne pourrait pas atteindre la portion de la conjuguée $C = -\frac{1}{\sqrt[3]{2}}$ qui contient les points dangereux imaginaires; c'est-à-dire qu'on ne voit pas tout d'abord auquel des trois points A, D, D′ la région de convergence de la série sera limitée. A la vérité, ce serait incontestablement au point A, si

$$(\alpha_0 - a\sqrt[3]{4})^2 + \beta_0^2$$

se trouvait à la fois moindre que

$$\left(\alpha_0 + \frac{a\sqrt[3]{4}}{2}\right)^2 + \left(\beta_0 + \frac{a\sqrt[3]{4}\sqrt{3}}{2}\right)^2,$$

et que

$$\left(\alpha_0 + \frac{a\sqrt[3]{4}}{2}\right)^2 + \left(\beta_0 + \frac{a\sqrt[3]{4}\sqrt[2]{3}}{2}\right)^2,$$

inégalités qui se réduisent à

$$\alpha_0\sqrt{3} + \beta_0 > 0$$

et

$$\alpha_0\sqrt[2]{3} - \beta_0 > 0;$$

mais elles ne seraient satisfaites ni l'une ni l'autre, que la région de convergence n'en serait pas moins encore bornée au point A, laissant à l'écart les points D et D' à des distances plus ou moins considérables.

En effet, imaginons que nous revenions à l'un des points qui, ayant son abscisse définie par les équations

$$\alpha_0 = a\sqrt[3]{4}, \quad a\sqrt[3]{4}\sqrt[2]{3} \pm \beta_0 = 0,$$

appartiendrait d'ailleurs à une portion de conjuguée tangente à la courbe réelle en un point de l'arc OBSA.

Il est acquis que si nous diminuions infiniment peu $\alpha_0$, sans faire varier $\beta_0$, la région de convergence n'atteindrait même plus alors la portion de la conjuguée $C = \infty$ qui passe en A; comment pourrait-on donc concevoir que si, au contraire, on augmentait infiniment peu $\alpha_0$, la région de convergence prît instantanément un développement qui en portât la limite au delà de l'un des points D ou D'?

Au reste, les deux conditions

$$\alpha_0\sqrt{3} \pm \beta_0 > 0$$

sont pleinement remplies lorsque le point de départ appartient à la portion de la conjuguée $C = \infty$ qui touche la courbe réelle en A; comment pourrait-on donc concevoir que la région de convergence limitée précédemment en A, lorsque $\alpha_0$ était compris entre $\frac{a}{\sqrt{2}}$ et $a\sqrt[3]{4}$, le point de départ appartenant alors à une branche de conjuguée tangente

à la courbe réelle en un point de l'arc OBSA, et restant encore limitée au même point lorsque le point de départ vient se placer sur la portion de la conjuguée $C = \infty$ qui touche la courbe réelle en A, eût pu dans l'intervalle s'étendre jusqu'à l'un des deux points D ou D′ qu'elle aurait au contraire dû toujours tendre à absorber en enveloppant une portion de plus en plus grande de l'espace répandu autour d'eux?

Les choses ne se passent jamais d'une façon à ce point extraordinaire; et quant au fait même qui nous occupe, il trouvera une explication bien simple dans l'observation suivante : à chacune des valeurs particulières de $x$,

$$a\sqrt[3]{4}\,\frac{-1-\sqrt{3}\sqrt{-1}}{2},\quad a\sqrt[3]{4}\,\frac{-1+\sqrt{3}\sqrt{-1}}{2},$$

il correspond, pour $y$, les valeurs doubles

$$a\sqrt[3]{2}\,\frac{-1+\sqrt{3}\sqrt{-1}}{2},\quad a\sqrt[3]{2}\,\frac{-1-\sqrt{3}\sqrt{-1}}{2},$$

qui sont les ordonnées des points dangereux D et D′, et des valeurs simples

$$a\sqrt[3]{2}(1-\sqrt{3}\sqrt{-1}),\quad a\sqrt[3]{2}(1+\sqrt{3}\sqrt{1}),$$

qui sont les ordonnées de points ne présentant aucune particularité remarquable. Or ce n'est évidemment qu'à l'un de ces points, et non à l'un des points D ou D′, que peut se rendre le point $[x, y]$, lorsque $\alpha_0$ dépassant $a\sqrt[3]{4}$, et $\alpha_0\sqrt[2]{3} \pm \beta_0$ étant négatifs, le point de départ appartient d'ailleurs à une branche de conjuguée tangente à la courbe réelle en un point de l'arc OBSA.

L'égalité momentanée des distances modulaires du point de départ aux points A et D ou D′, quand $\alpha_0\sqrt{3} \pm \beta = 0$, ne signifie donc en aucune façon que la limite de la région de convergence passe à la fois au point A et à l'un des points D ou D′, mais bien qu'elle passe au point A et à l'un des points qui, ayant leurs abscisses égales à celles des points D et D′, ne présentent toutefois aucune particularité remarquable.

La fausse indication fournie par la condition de convergence tient

encore, dans ce cas, à ce que l'ordonnée du point de départ n'y entre pas : lorsque le point de départ appartiendra à une branche de conjuguée tangente à la courbe réelle en un point de l'arc AOT', la même indication, dans les mêmes circonstances,

$$\alpha_0\sqrt{3} \pm \beta_0 = 0$$

deviendra exacte.

La même difficulté apparente, si l'on eût voulu l'apercevoir, se serait déjà présentée lorsque le point de départ appartenait à une branche de conjuguée tangente à l'arc TO : si, par exemple, on avait pris pour point de départ le point de cet arc, qui, ayant pour abscisse $\frac{a\sqrt[3]{4}}{2}$ ou $\frac{a}{\sqrt[3]{2}}$, se trouverait sur une verticale menée à égale distance de l'axe des $y$ et de la tangente au point A, les distances modulaires du point de départ à l'origine et au point A se seraient trouvées égales ; mais il n'eût évidemment pas fallu en conclure que la limite de la région de convergence dût alors passer à la fois à l'origine et au point A : elle aurait passé par l'origine et par le point

$$x = a\sqrt[3]{4},$$
$$y = -2a\sqrt[3]{2}.$$

C'est par les mêmes motifs que chacun des points du lieu $\alpha = 0$ paraissait également éloigné des deux points dangereux du lieu

$$y^3 - a^2 y + a^2 x = 0;$$

$\alpha_0$ devenant nul sans que $\alpha'_0$ le fût, la limite de la région de convergence passait à l'un des points dangereux et au point simple qui avait même abscisse que l'autre.

Supposons maintenant que le point de départ marchant toujours dans le même sens se rende sur les conjuguées qui touchent l'arc AOT' de la courbe réelle.

La région de convergence restera d'abord limitée au point A, parce que sur les conjuguées dont le contact aurait lieu très-près de A, on ne pourra pas trouver de points remplissant l'une ou l'autre des con-

ditions
$$\alpha_0 \pm \beta_0 < 0.$$

Tant que le point A restera sur la limite de la région de convergence, il ne pourra arriver au point $[x, y]$ que de passer sur la courbe réelle, sur la portion de la conjuguée $C = \infty$ qui passe au point A ou sur la portion de la conjuguée $C = 0$ qui passe à l'origine. On constatera ces diverses circonstances, comme dans le cas précédent, et l'on pourra par conséquent assigner par les mêmes moyens la valeur finale de $y$; nous n'insisterons donc pas sur ce cas.

Supposons enfin que le point de départ appartienne à une conjuguée assez éloignée du point A pour qu'on y puisse trouver des points tels, que
$$\alpha_0 \pm \beta_0 \text{ soit négatif},$$
de façon que la région de convergence soit alors limitée à l'un des points D ou D'.

Les distances modulaires du point de départ à ces deux points étant
$$\left(\alpha_0 + \frac{a\sqrt[3]{4}}{2}\right)^2 + \left(\beta_0 + \frac{a\sqrt[3]{4}\sqrt[2]{3}}{2}\right)^2$$
et
$$\left(\alpha_0 + \frac{a\sqrt[3]{4}}{2}\right)^2 + \left(\beta_0 - \frac{a\sqrt[3]{4}\sqrt[2]{3}}{2}\right)^2,$$
on voit que la région de convergence sera limitée au point D ou au point D' suivant que $\beta_0$ sera négatif ou positif, c'est-à-dire suivant que le point de départ appartiendra à l'une ou à l'autre des deux branches de la conjuguée, où il se trouve, qui partent de la courbe réelle. Si le point de départ appartenait à la courbe réelle (il faudrait alors qu'il fût à la gauche de l'origine pour que $\alpha_0 \pm \beta_0$ fût négatif), la limite de la région de convergence passerait à la fois aux deux points D et D'.

Dans le cas qui nous occupe, deux des valeurs de $y$ correspondantes à la valeur finale de $x$ pourraient ne se distinguer l'une de l'autre que par le signe des parties imaginaires des valeurs qu'elles fourniraient pour
$$\frac{dy}{dx};$$

mais on saura toujours quel signe aura dû prendre la partie imaginaire de $\frac{dy}{dx}$ au point d'arrivée, si l'on a relevé les passages du point $[x, y]$ sur l'enveloppe imaginaire.

Cette enveloppe est définie par la condition

$$\frac{ay - x^2}{y^2 - ax} = \text{réel},$$

ou

$$\frac{a\alpha' - \alpha^2 + \beta^2}{\alpha'^2 - \beta'^2 - a\alpha} = \frac{a\beta' - 2\alpha\beta}{2\alpha'\beta' - a\beta},$$

d'où l'on pourrait éliminer $\alpha'$ et $\beta'$, ce qui fournirait entre $\alpha$ et $\beta$ une équation

$$\varphi(\alpha, \beta) = 0.$$

Le point $[x, y]$ aurait ou n'aurait pas passé sur l'enveloppe, suivant que

$$\varphi(\alpha_0, \beta_0)\,\varphi(\alpha_1, \beta_1)$$

aurait le signe $-$ ou le signe $+$. Le calcul de l'équation

$$\varphi(\alpha, \beta) = 0$$

ne présentant aucune difficulté théorique, nous ne nous y arrêtons pas.

*De l'intégration par série.*

**116.** Nous nous occuperons ici seulement des équations où n'entre pas la variable dépendante, qui, par conséquent, se présentent sous la forme

$$f\left(x, \frac{dy}{dx}\right) = 0$$

ou plus généralement

$$f\left(x, \frac{d^n y}{dx^n}\right) = 0.$$

L'intégration, par la série de Taylor, d'une équation de la forme

$$f\left(x, \frac{dy}{dx}\right) = 0,$$

présentait des difficultés qui rendaient peu sûr l'emploi de cette méthode : et ce n'est pas de l'incertitude qui pesait encore sur la limite de la région de convergence que j'entends parler ici, car, en évitant tous les points dangereux indistinctement, on pouvait du moins être certain que la série employée resterait convergente. En sorte qu'ayant développé $\frac{dy}{dx}$ et par suite, par intégration, $y$, de la limite inférieure $x_0$, numérique, à une limite variable $x_1$, telle que le module de $(x_1 - x_0)$ ne dépassât pas une certaine quantité $R_0$, on pouvait attribuer à $x_1$ l'une des valeurs que cette variable pouvait prendre, développer de nouveau $\frac{dy}{dx}$, et par suite $y$, de la valeur numérique $x_1$ à une nouvelle limite variable $x_2$ telle que le module de $(x_2 - x_1)$ ne dépassât pas une nouvelle quantité $R_1$, et ainsi de suite, ce qui eût fourni pour $y$ une expression de la forme

$$\begin{aligned}
y = y_0 &+ \left(\frac{dy}{dx}\right)_0 \frac{x_1 - x_0}{1} + \left(\frac{d^2y}{dx^2}\right)_0 \frac{(x_1 - x_0)^2}{1.2} + \ldots \\
&+ \left(\frac{dy}{dx}\right)_1 \frac{x_2 - x_1}{1} + \left(\frac{d^2y}{dx^2}\right)_1 \frac{(x_2 - x_1)^2}{1.2} + \ldots \\
&+ \left(\frac{dy}{dx}\right)_2 \frac{x_3 - x_2}{1} + \left(\frac{d^2y}{dx^2}\right)_2 \frac{(x_3 - x_2)^2}{1.2} + \ldots \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&+ \left(\frac{dy}{dx}\right)_n \frac{x_{n+1} - x_n}{1} + \left(\frac{d^2y}{dx^2}\right)_n \frac{(x_{n+1} - x_n)^2}{1.2} + \ldots;
\end{aligned}$$

puisque la constante, introduite dans chaque nouvelle intégration, devait avoir pour valeur celle que l'intégration précédente avait donnée pour $y$.

Mais, en premier lieu, s'il eût fallu recourir à la sommation effective des suites précédentes, pour former la valeur initiale de $\left(\frac{dy}{dx}\right)$, qui devait servir à composer la nouvelle suite qu'on eût voulu ajouter au dé-

veloppement, la longueur des calculs d'abord, mais surtout l'incertitude qui eût nécessairement pesé sur les résultats à obtenir, eussent fait renoncer à l'emploi de cette méthode.

En second lieu, et ce point a beaucoup plus d'importance, on n'eût pu, en tout cas, régler les étapes de $x$ de manière à pouvoir répondre d'obtenir successivement ou séparément toutes ou chacune des $m^2$ valeurs de $y$ dont les dérivées, au départ, représentées par les différentes racines de l'équation

$$f\left(x_0, \frac{dy}{dx}\right) = 0,$$

seraient devenues, à l'arrivée, celles de l'équation

$$f\left(x_{n+1}, \frac{dy}{dx}\right) = 0.$$

On eût bien pu, pour former la première suite, prendre successivement pour $\left(\frac{dy}{dx}\right)_0$ toutes les racines de l'équation

$$f\left(x_0, \frac{dy}{dx}\right) = 0$$

et avancer de proche en proche vers $x_{n+1}$; mais on manquait d'une règle qui permît de prévoir sur quelle valeur de $\left(\frac{dy}{dx}\right)_{n+1}$ on tomberait à la fin du calcul. On pouvait bien recommencer en adoptant de nouvelles étapes pour $x$, mais on ne pouvait pas être assuré de ne pas retomber toujours sur les mêmes combinaisons. Enfin, si quelques nouveaux essais avaient successivement conduit à de nouvelles combinaisons, on n'avait pas de règle certaine pour parvenir à celles qui se seraient dérobées jusque-là.

Ces difficultés n'existent plus maintenant.

En premier lieu, quand on aura formé les $p$ premières suites qui, conformément à la marche adoptée, devront fournir le développement de $y$, de $x_0$ à $x_p$, au lieu de calculer la valeur de $\left(\frac{dy}{dx}\right)_p$, qui doit

concourir à la formation de la $p+1^{ième}$ suite, par la sommation directe de

$$\left(\frac{dy}{dx}\right)_0 + \left(\frac{d^2y}{dx^2}\right)_0 \frac{x_1 - x_0}{1} + \left(\frac{d^3x}{dx^3}\right)_0 \frac{(x_1 - x_0)^2}{1.2} + \ldots$$
$$+ \left(\frac{d^2y}{dx^2}\right)_1 \frac{x_2 - x_1}{1} + \left(\frac{d^3y}{dx^3}\right)_1 \frac{(x^2 - x_1)^2}{1.2} + \ldots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$+ \left(\frac{d^2y}{dx^2}\right)_{p-1} \frac{x_p - x_{p-1}}{1} + \left(\frac{d^3y}{dx^3}\right)_{p-1} \frac{(x_p - x_{p-1})^2}{1.2} + \ldots,$$

on la tirera de l'équation

$$f\left(x_p \frac{dy}{dx}\right) = 0,$$

qui la fournira plus aisément et avec une approximation dont, au moins, on pourra répondre.

En second lieu, la méthode que nous avons donnée pour reconnaître parmi les racines de l'équation

$$f(x_p, y) = 0$$

celle que représente le développement, suivant la série de Taylor, de la fonction, de $x_{p-1}$ à $x_p$, cette méthode est évidemment réciproque, c'est-à-dire qu'on pourra en renverser l'emploi et choisir $x_p$ de manière que le point d'arrivée $[x_p, y_p]$ satisfasse à telle condition donnée qu'il pourrait remplir, qu'il se trouve, par exemple, sur une conjuguée désignée que rencontre la région de convergence.

On pourra ainsi, par étapes réglées à l'avance, amener le point $[x, y]$ du point $[x_0, y_0]$ à celui des points $[x_{n+1}, y]$ que l'on voudra.

En déterminant ainsi les $m^2$ chemins que $x$ devrait suivre successivement pour que $\frac{dy}{dx}$ parvînt de chacune de ses $m$ valeurs qui correspondent à $x_0$ à chacune de ses $m$ valeurs qui correspondent à $x_{n+1}$ ($n$ est ici un nombre variable, mais $x_{n+1}$ est la valeur finale de $x$), on obtiendra les $m^2$ intégrales de l'équation proposée; $x_{n+1}$ y représentera une variable assujettie à des conditions d'inégalité différentes dans des intégrales différentes.

La même méthode s'appliquerait évidemment à une équation différentielle d'ordre supérieur.

$$f\left(x, \frac{d^n y}{dx^n}\right) = 0,$$

les $m^2$ intégrales de cette équation contiendraient comme constantes arbitraires $y_0, \left(\frac{dy}{dx}\right)_0, \ldots, \left(\frac{d^{n-1} y}{dx^{n-1}}\right)_0$. Mais le calcul arithmétique des valeurs de $\left(\frac{dy}{dx}\right)_p, \left(\frac{d^2 y}{dx^2}\right)_p, \ldots, \left(\frac{d^{n-1} y}{dx^{n-1}}\right)_p, \left(\frac{d^n y}{dx^n}\right)_p$, nécessaire à la formation de la $p+1^{ième}$ suite, ne se ferait plus aussi simplement que dans le cas précédent.

$\left(\frac{d^n y}{dx^n}\right)_p$ serait bien toujours fourni par l'équation

$$f\left(x_p, \frac{d^n y}{dx^n}\right) = 0.$$

Mais $\left(\frac{d^{n-1} y}{dx^{n-1}}\right)_p, \ldots, \left(\frac{dy}{dx}\right)_p$ devraient être séparément calculés par la sommation directe des suites qui les représenteraient et qu'on aurait formées précédemment par intégrations répétées du développement de $\frac{d^n y}{dx^n}$.

Prenons pour exemple l'équation

$$\left(\frac{dy}{dx}\right)^3 - a^2\left(\frac{dy}{dx}\right) + a^2 x = 0,$$

dont l'intégrale générale fournirait la quadrature de la courbe

$$z^3 - a^2 z + a^2 x = 0$$

et de ses conjuguées.

Si l'on voulait intégrer $y$ entre des limites

$$x_0, \quad \left(\frac{dy}{dx}\right)_0 = z_0 \qquad \text{et} \qquad x, \quad \left(\frac{dy}{dx}\right) = z,$$

correspondantes à des points du lieu

$$z^3 - a^2 z + a^2 x = 0,$$

situés l'un sur une branche d'une conjuguée tangente à la courbe

réelle en un point de l'arc LM (*fig.* 7) et l'autre sur une branche d'une conjuguée tangente à la branche L'N, ce qui serait le plus grand écart possible, on prendrait les points intermédiaires successifs sur des conjuguées dont les points de contact avec la courbe réelle marchassent dans le sens MLOL'N, en évitant, pour plus de simplicité, les conjuguées tangentes à l'enveloppe imaginaire, puisqu'il ne servirait à rien d'y passer d'abord, pour en sortir ensuite.

Cela obligerait à passer par l'origine des coordonnées pour changer de demi-conjuguée. Quand on serait près du point d'arrivée, on repasserait ou non une dernière fois sur la courbe réelle, suivant que l'avant-dernière station et la dernière seraient en des points situés de côtés différents ou du même côté, sur leurs conjuguées respectives, par rapport aux points de contact de ces conjuguées avec la courbe réelle.

*De l'intégration par approximation.*

**117.** L'intégration par la série de Taylor avait sur les autres méthodes d'intégration par approximation cet avantage considérable que, la série représentant, au moins entre de certaines limites, la fonction intégrale, on pouvait y donner aussi bien à la variable des valeurs imaginaires que des valeurs réelles; tandis que les formules anciennement connues de quadratures approchées n'étaient applicables qu'au cas où les valeurs extrêmes de la variable indépendante se trouvaient réelles.

Ce motif de préférence n'existe plus aujourd'hui et je crois qu'on parviendrait, dans la plupart des cas, plus rapidement et plus sûrement à la valeur de l'intégrale cherchée en carrant, suivant les principes établis au chapitre III, les deux conjuguées qui passeraient par les limites, et l'enveloppe (lorsque cela se pourrait), au moyen des formules de Simpson ou de M. Poncelet.

Ces méthodes fourniraient d'ailleurs à volonté des limites inférieures et des limites supérieures de chaque partie de l'intégrale, de façon qu'on pût toujours juger du degré d'approximation du résultat obtenu, ce qui ne peut guère se faire quand on n'a d'autre moyen pour y parvenir que la sommation des termes de la série.

# THÉORÈMES

CONCERNANT

## LE QUADRUPLE D'UN NOMBRE PREMIER DE LA FORME $12k+5$;

### PAR M. J. LIOUVILLE.

Désignons par $m$ un nombre premier donné, de la forme $12k+5$: considérons son quadruple $4m$, et posons de toutes les manières possibles l'équation

$$4m = x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs et $p$ un nombre premier qui ne divise pas $y$ : on admet pour $l$ la valeur zéro. Nous trouvons tout de suite par nos *formules générales* que le nombre N des décompositions de $4m$ ainsi obtenues est essentiellement pair; mais comme on compte zéro parmi les nombres pairs, le cas de $N=0$ ne serait pas exclu. Or une analyse plus délicate fait voir que N est la somme de deux nombres impairs $N_1$, $N_2$, et dès lors on est sûr d'avoir soit $N=2$, soit $N>2$

On peut, en effet, distinguer dans l'équation

$$4m = x^2 + p^{4l+1}y^2$$

deux genres de solutions, suivant que $x$ est ou n'est pas divisible par 3. Dans le premier cas, on a, vu la forme donnée de $m$,

$$p \equiv 2 \pmod{3},$$

tandis que dans le second cas on a au contraire

$$p \equiv 1 \pmod{3}.$$

D'ailleurs $p$ vérifie toujours la congruence

$$p \equiv 3 \pmod{8}.$$

Il s'ensuit que $p$ est de la forme

$$24g + 11$$

lorsque $x$ est multiple de 3, mais de la forme

$$24g + 19$$

lorsque $x$ est premier à 3. Quant à $y$, il n'est jamais divisible par 3.

Ceci expliqué, nous pouvons énoncer les deux théorèmes suivants, qui montreront comment N est la somme de deux entiers impairs $N_1$, $N_2$, respectivement relatifs aux deux genres de décompositions de $4m$ dont nous venons de parler.

*Théorème I.* — Pour chaque nombre premier $m$, de la forme $12k + 5$, on peut poser au moins une fois (et toujours un nombre impair de fois) l'équation

$$4m = 9x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs et $p$ un nombre premier $24g + 11$ qui ne divise pas $y$.

En d'autres termes, si du quadruple d'un nombre premier donné, de la forme $12k + 5$, on retranche, tant que faire se peut, les carrés

$$9,\ 81,\ 225, \ldots,$$

des nombres impairs multiples de 3, il y aura un nombre impair de restes susceptibles d'être mis sous la forme

$$p^{4l+1}y^2,$$

$p$ étant un nombre premier non diviseur de $y$ et naturellement de la forme $24g + 11$

*Théorème II.* — Pour chaque nombre premier $m$, de la forme $12k+5$, on peut poser au moins une fois (et toujours un nombre impair de fois) l'équation

$$4m = x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs non divisibles par 3, et $p$ un nombre premier $24g+19$ qui ne divise pas $y$.

En d'autres termes, si du quadruple d'un nombre premier donné, de la forme $12k+5$, on retranche, tant que faire se peut, les carrés

$$1,\ 25,\ 49,\ 121, \ldots,$$

des nombres impairs premiers à 3, il y aura un nombre impair de restes susceptibles d'être mis sous la forme

$$p^{4l+1}y^2,$$

$p$ étant un nombre premier non diviseur de $y$ et naturellement de la forme $24g+19$. La condition relative de $y$ (de ne pas être un multiple de 3) sera remplie d'elle-même.

Passons aux exemples, et d'abord soit

$$m = 5:$$

nous aurons l'équation

$$4.5 = 9.1^2 + 11.1^2,$$

conformément au théorème I, et l'équation

$$4.5 = 1^2 + 19.1^2,$$

conformément au théorème II.

En prenant $k=1$, la formule $12k+5$ nous donne le nombre premier 17, et là encore nos théorèmes sont vérifiés, puisque l'on a d'une part

$$4.17 = 9.1^2 + 59.1^2,$$

et d'autre part

$$4.17 = 1^2 + 67.1^2,$$
$$4.17 = 5^2 + 43.1^2,$$
$$4.17 = 7^2 + 19.1^2.$$

Enfin, pour

$$m = 12.2 + 5 = 29,$$

même vérification; on n'a alors que les deux équations canoniques ci-après, une pour chaque genre :

$$4.29 = 9.1^2 + 107.1^2$$

et

$$4.29 = 7^2 + 67.1^2.$$

Ces exemples suffiront. Mais en terminant faisons observer que notre décomposition en deux entiers impairs $N_1$, $N_2$ du nombre complet (et essentiellement pair) N des solutions de l'équation

$$4m = x^2 + p^{4l+1}y^2,$$

où l'on confondrait les deux espèces de valeurs de $x^2$ (mod. 3) ou de $p$ (mod. 3), n'est pas sans quelque analogie avec la distinction des formes quadratiques en *genres*, qui joue un si grand rôle dans la théorie de ces formes.

# THÉORÈMES

CONCERNANT

## RESPECTIVEMENT LES NOMBRES PREMIERS DE LA FORME $16k+3$ ET LES NOMBRES PREMIERS DE LA FORME $16k+11$;

PAR M. J. LIOUVILLE.

1. La forme linéaire $8\mu+3$ se décompose dans les deux suivantes $16k+3$, $16k+11$, au sujet desquelles nous voulons présenter deux théorèmes qui nous semblent curieux. Mais d'abord observons que pour tout nombre premier $m$ de la forme $8\mu+3$, on peut écrire (d'une seule manière) en nombres entiers :

$$m = a^2 + 2b^2.$$

Comme, d'ailleurs, $a$ et $b$ ne peuvent être qu'impairs, si l'on fait

$$\frac{a^2-b^2}{8} = n,$$

le quotient $n$ sera entier. Dans tout le cours de cet article, nous conserverons à $m$ et à $n$ la signification que nous venons de leur attribuer. Ainsi $m$ désignera toujours un nombre premier $8\mu+3$; mais nous supposerons successivement $\mu$ pair ($\mu = 2k$), puis $\mu$ impair ($\mu = 2k+1$), ce qui donnera au nombre $m$ les deux formes $16k+3$, $16k+11$, sans que les équations fondamentales

$$m = a^2 + 2b^2$$

et

$$n = \frac{a^2-b^2}{8}$$

cessent d'avoir lieu. Ajoutons que nous n'aurons pas besoin de la valeur même de $n$, mais seulement de la valeur de $n$ (mod. 2). Or il est

clair que $n$ est pair quand $a$ et $b$ sont tous les deux compris dans la formule $8\nu \pm 1$, ou tous les deux compris dans la formule $8\nu \pm 3$ : au contraire $n$ est impair quand un des deux entiers $a$, $b$ appartient à la formule $8\nu \pm 1$ et l'autre à la formule $8\nu \pm 3$.

2. Commençons par les nombres premiers $16k + 3$, et désignant par $m$ un nombre donné de cette espèce, posons de toutes les manières possibles l'équation

$$m = (8t + 3)^2 + 2p^{4l+1}y^2,$$

$t$ désignant un entier indifféremment pair ou impair, positif, nul ou négatif, tandis que $y$ et $p$ sont impairs et positifs, de plus $p$ premier (naturellement de la forme $4\nu + 1$) et non diviseur de $y$. On demande une règle facile qui dise à priori si le nombre N des décompositions de $m$ sous la forme indiquée est pair ou impair.

Or je réponds à cette question par la congruence

$$N \equiv n \pmod{2},$$

le nombre $n$ étant celui qu'on a défini plus haut.

Les valeurs successives de

$$(8t + 3)^2,$$

où $t$ est indifféremment pair ou impair, positif, nul ou négatif, sont

$$3^2,\ 5^2,\ 11^2,\ 13^2,\ldots;$$

d'après cela, on vérifiera aisément notre théorème sur les nombres premiers

$$3,\ 19,\ 67,\ 83,\ldots,$$

que la formule $16k + 3$ fournit.

Bornons-nous aux quatre plus petits. On a

$$3 = 1^2 + 2.1^2,$$
$$19 = 1^2 + 2.3^2,$$
$$67 = 7^2 + 2.3^2,$$
$$83 = 9^2 + 2.1^2:$$

$n$ est donc pair pour le premier et le dernier d'entre eux, mais impair pour les deux autres. Or cela est vrai aussi de N. D'abord pour $m=3$, on a évidemment $N=0$; mais pour $m=19$, on a la décomposition canonique

$$19=3^2+2.5.1^2;$$

67 aussi en offre une, savoir

$$67=3^2+2.29.1^2.$$

Enfin pour $m=83$, on retrouve N pair, $N=2$, les équations canoniques étant alors

$$83=3^2+2.37.1^2,$$
$$83=5^2+2.29.1^2.$$

Notre théorème a donc toujours lieu.

3. Passons aux nombres premiers $16k+11$; et désignant par $m$ un nombre donné de cette espèce, posons de toutes les manières possibles l'équation

$$m=(8t+1)^2+2p^{4l+1}y^2,$$

où l'on prendra $t$ indifféremment pair ou impair, positif, nul ou négatif, tandis que $y$ et $p$ seront impairs et positifs, de plus $p$ premier (naturellement de la forme $4\nu+1$) et non diviseur de $y$. Cette fois encore, il s'agit de décider si le nombre N des décompositions de $m$ sous la forme indiquée est pair ou impair, et c'est encore par la congruence

$$N\equiv n \pmod{2}$$

que je réponds à cette question.

Les valeurs successives de

$$(8t+1)^2,$$

où $t$ est indifféremment pair ou impair, positif, nul ou négatif, sont

$$1^2,\ 7^2,\ 9^2,\ 15^2,\ldots;$$

d'après cela, on vérifiera aisément notre théorème sur les nombres premiers

$$11,\ 43,\ 59,\ 107,\ldots,$$

que la formule $16k + 11$ fournit.

Bornons-nous aux quatre plus petits. On a

$$11 = 3^2 + 2.1^2,$$
$$43 = 5^2 + 2.3^2,$$
$$59 = 3^2 + 2.5^2,$$
$$107 = 3^2 + 2.7^2;$$

$n$ est donc impair pour 11 et 107, mais pair pour 43 et 59. Or il en est ainsi de N. En effet, on a pour 11 la décomposition canonique

$$11 = 1^2 + 2.5.1^2.$$

Mais pour 43, on n'en a aucune; et, pour 59, on en a deux

$$59 = 1^2 + 2.29.1^2,$$
$$59 = 7^2 + 2.5.1^2.$$

Enfin pour $m = 107$, on retrouve N impair, $N = 3$, comme le montrent les équations

$$107 = 1^2 + 2.53.1^2,$$
$$107 = 7^2 + 2.29.1^2,$$
$$107 = 9^2 + 2.13.1^2.$$

Notre théorème a donc toujours lieu.

# THÉORÈME

## CONCERNANT LES NOMBRES PREMIERS DE LA FORME $24k+13$;

**Par M. J. LIOUVILLE.**

Le théorème que nous voulons énoncer ici, au sujet des nombres premiers de la forme $24k+13$, consiste en ce que pour chaque nombre donné $m$, de cette espèce, on peut poser au moins une fois, et toujours un nombre impair de fois, l'équation

$$m = 6x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs, et $p$ un nombre premier $(24g+7)$ qui ne divise pas $y$ : on admet pour $l$ la valeur zéro.

En d'autres termes, si d'un nombre premier donné $m$, de la forme $24k+13$, on retranche, tant que faire se peut, le sextuple des carrés des nombres impairs 1, 3, etc., il y aura un nombre impair de restes susceptibles d'être mis sous la forme

$$p^{4l+1}y^2,$$

$p$ étant un nombre premier non diviseur de $y$. Quant à la forme linéaire $(24g+7)$ que nous attribuons à $p$, c'est une conséquence immédiate de l'équation

$$m = 6x^2 + p^{4l+1}y^2,$$

qui, dans les conditions où nous nous sommes placés, entraîne ces deux congruences

$$p \equiv 7 \pmod{8}$$

et

$$p \equiv 1 \pmod{3}.$$

Le nombre premier le plus petit que la formule

$$24k + 13$$

puisse nous offrir est 13. Or on a

$$13 = 6.1^2 + 7.1^2,$$

ce qui s'accorde avec notre théorème, le nombre premier 7 se déduisant de la formule

$$24g + 7,$$

en y prenant $g = 0$.

En prenant $k = 1$, on a encore un nombre premier, savoir 37, et l'équation canonique

$$37 = 6.1^2 + 31.1^2.$$

Soit à présent $k = 2$, d'où $m = 61$; c'est encore un nombre premier, et l'on a encore une seule équation canonique :

$$61 = 6.3^2 + 7.1^2.$$

En posant $k = 3$, on trouverait un nombre composé; mais pour $k = 4$, on a le nombre premier 109, et l'équation canonique

$$109 = 6.1^2 + 103.1^2.$$

Toujours notre théorème est vérifié.

# THÉORÈME

## CONCERNANT LES NOMBRES PREMIERS DE LA FORME $24k+1$;

PAR M. J. LIOUVILLE.

Soit $m$ un nombre premier de la forme $24k+1$. Je pose de toutes les manières possibles l'équation

$$m = 12x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs et $p$ un nombre premier qui ne divise pas $y$ : j'admets pour $l$ la valeur zéro. On demande une règle simple qui dise à priori si le nombre N des décompositions de $m$ sous la forme indiquée est pair ou impair.

Nous répondrons à cette question en remarquant que pour tout nombre premier $m$ de la forme $24k+1$, on peut poser, d'une seule manière, en nombres entiers, l'équation

$$m = a^2 + 24b^2,$$

et en ajoutant que l'on a toujours

$$\mathrm{N} \equiv b \pmod{2},$$

en sorte que N est pair quand $b$ est pair, mais impair quand $b$ est impair. Nous n'avons pas besoin d'avertir que zéro est compté comme nombre pair.

Les quatre nombres premiers les plus petits que la formule $24k+1$ fournisse sont

$$73 = 7^2 + 24.1^2,$$
$$97 = 1^2 + 24.2^2,$$
$$193 = 13^2 + 24.1^2,$$
$$241 = 5^2 + 24.3^2.$$

Pour le second de ces nombres, $b$ est pair, N doit donc aussi l'être. Pour les trois autres, $b$ étant impair, N doit être impair. Or il est aisé, en effet, de s'assurer que notre équation

$$m = 12x^2 + p^{4l+1}y^2$$

est impossible pour $m = 97$, de façon qu'alors $N = 0$, tandis que l'on a $N = 1$, relativement aux trois autres valeurs de $m$ citées plus haut 73, 193, 241; c'est ce que prouve pour 73 l'équation canonique

$$73 = 12.1^2 + 61.1^2,$$

puis pour 193 et 141 les équations canoniques respectives

$$193 = 12.1^2 + 181.1^2$$

et

$$241 = 12.1^2 + 229.1^2.$$

Il est bon de faire observer que les nombres premiers qui figurent aux seconds membres des équations que nous venons d'écrire sont tous de la forme $24g + 13$. C'est qu'en effet, dans les conditions où nous nous sommes placés, l'équation

$$m = 12x^2 + p^{4l+1}y^2$$

entraîne les deux congruences

$$p \equiv 5 \pmod{8}$$

et

$$p \equiv 1 \pmod{3},$$

d'où résulte nécessairement

$$p = 24g + 13.$$

# THÉORÈME

## CONCERNANT LES NOMBRES PREMIERS DE LA FORME $40\mu + 3$;

**Par M. J. LIOUVILLE.**

---

Soit $m$ un nombre premier donné, de la forme $40\mu + 3$. Posons de toutes les manières possibles l'équation

$$m = (10t + 3)^2 + 2p^{4l+1}y^2,$$

$t$ étant un entier indifféremment pair ou impair, positif, nul ou négatif, tandis que $y$ et $p$ sont impairs et positifs, de plus $p$ premier et non diviseur de $y$ : nous admettons pour $l$ la valeur zéro. On demande une règle facile qui dise à priori si le nombre N des décompositions de $m$ ainsi obtenues est pair ou impair, zéro étant compté comme nombre pair.

Pour répondre à cette question, j'observe que le nombre premier $m$ étant de la forme $40\mu + 3$ est $\equiv 3$ (mod. 8) et que par conséquent on peut poser, d'une seule manière, en nombres entiers,

$$m = a^2 + 2b^2.$$

Or tout dépend ici de la valeur de $a$ (mod. 5); car N est impair quand $a$ est divisible par 5, mais pair quand $a$ est premier à 5.

Les entiers fournis par la formule générale

$$(10t + 3)^2$$

en y faisant successivement $t = 0$, $t = \pm 1$, $t = \pm 2, \ldots$, sont

$$3^2,\ 7^2,\ 13^2,\ 17^2,\ 23^2, \ldots;$$

vérifions, d'après cela, notre théorème en prenant pour $m$ les nombres

premiers $40\mu + 3$ les plus petits, savoir

$$3,\ 43,\ 83,\ 163,\ 283.$$

Comme on a

$$3 = 1^2 + 2.1^2,$$
$$43 = 5^2 + 2.3^2,$$
$$83 = 9^2 + 2.1^2,$$
$$163 = 1^2 + 2.9^2,$$
$$283 = 11^2 + 2.9^2,$$

ce qui donne pour $a$ les valeurs respectives

$$1,\ 5,\ 9,\ 1,\ 11,$$

on voit que N doit être impair pour 43, mais pair pour 3, 83, 163 et 283. Or on trouve en effet $N = 1$ pour $m = 43$, en vertu de l'équation canonique

$$43 = 3^2 + 2.17.1^2,$$

tandis que l'on a $N = 0$ pour $m = 3$ et $m = 163$, et $N = 2$ pour $m = 83$ et $m = 283$, les équations canoniques étant, dans ces deux derniers exemples,

$$83 = 3^2 + 2.37.1^2,$$
$$83 = 7^2 + 2.17.1^2,$$

puis

$$283 = 3^2 + 2.137.1^2,$$
$$283 = 7^2 + 2.13.3^2.$$

Le nombre premier $p$ qui figure au second membre de l'équation

$$m = (10t + 3)^2 + 2p^{4l+1}y^2$$

doit, dans les conditions où nous nous sommes placés, vérifier les deux congruences

$$p \equiv 1 \pmod{4}, \qquad p \equiv \pm 3 \pmod{5}.$$

Il est donc toujours de l'une ou de l'autre des deux formes $20g + 13$, $20g + 17$.

# THÉORÈME

## CONCERNANT LES NOMBRES PREMIERS DE LA FORME $40\mu+27$;

PAR M. J. LIOUVILLE.

Soit $m$ un nombre premier donné, de la forme $40\mu + 27$. Posons de toutes les manières possibles l'équation

$$m = (10t + 1)^2 + 2p^{4l+1}y^2,$$

$t$ étant un entier indifféremment pair ou impair, positif, nul ou négatif, tandis que $y$ et $p$ sont impairs et positifs, de plus $p$ premier et non diviseur de $y$ : nous admettons pour $l$ la valeur zéro. On demande une règle facile qui dise à priori si le nombre N des décompositions de $m$ est pair ou impair, zéro étant compté comme nombre pair.

Ici, comme pour la question analogue traitée dans l'article précédent pour les nombres premiers $40\mu + 3$, nous nous servirons de l'équation

$$m = a^2 + 2b^2$$

qui continue à avoir lieu, parce que les nombres premiers $40\mu + 27$ sont eux aussi $\equiv 3 \pmod{8}$. Et la conclusion sera la même, à savoir que, cette fois encore, N est impair quand $a$ est divisible par 5, mais pair quand $a$ est premier à 5.

Les entiers fournis par la formule générale

$$(10t + 1)^2,$$

en y faisant successivement $t = 0$, $t = \pm 1$, $t = \pm 2, \ldots$, sont

$$1^2,\ 9^2,\ 11^2,\ 19^2,\ 21^2, \ldots;$$

vérifions d'après cela notre théorème en prenant pour $m$ les nombres

premiers $40\mu + 27$ les plus petits, savoir :

$$67,\ 107,\ 227.$$

Comme on a

$$67 = 7^2 + 2.3^2,$$
$$107 = 3^2 + 2.7^2,$$
$$227 = 15^2 + 2.1^2,$$

ce qui donne pour $a$ les valeurs respectives

$$7,\ 3,\ 15,$$

on voit que N doit être impair pour 227, mais pair pour 67 et 107. Or on a, en effet, $N = 0$ pour $m = 67$; puis $N = 2$ pour $m = 107$, à cause des équations canoniques

$$107 = 1^2 + 2.53.1^2,$$
$$107 = 9^2 + 2.13.1^2;$$

enfin $N = 3$, pour $m = 227$ : dans ce dernier exemple, les équations canoniques sont

$$227 = 1^2 + 2.113.1^2,$$
$$227 = 9^2 + 2.73.1^2,$$
$$227 = 11^2 + 2.53.1^2.$$

Le nombre premier $p$ qui figure au second membre de l'équation

$$m = 40\mu + 27 = (10t + 1)^2 + 2p^{4l+1}y^2$$

doit évidemment vérifier les deux congruences

$$p \equiv 1 \pmod{4}, \qquad p \equiv \pm 3 \pmod{5};$$

il est donc, comme dans l'article précédent, de l'une ou de l'autre des deux formes $20g + 13$, $20g + 17$.

# THÉORÈMES

CONCERNANT

## LE QUINTUPLE D'UN NOMBRE PREMIER DE L'UNE OU DE L'AUTRE DES DEUX FORMES $40\mu+7$, $40\mu+23$;

**Par M. J. LIOUVILLE.**

Nous avons déjà donné (dans le cahier d'octobre 1860) deux théorèmes concernant respectivement les nombres premiers $40\mu+7$ et les nombres premiers $40\mu+23$ : l'énoncé changeait suivant qu'on s'occupait de l'une ou de l'autre de ces deux classes de nombres premiers. Ici, au contraire, nous mêlons les deux classes et nous considérons le quintuple $(5m)$ d'un nombre premier $m$ qui peut être indifféremment de la forme $40\mu+7$ ou de la forme $40\mu+23$ sans que nos énoncés changent.

*Théorème I.* — « Pour chaque nombre premier $m$, de l'une ou de » l'autre des deux formes $40\mu+7$, $40\mu+23$, on peut poser au » moins une fois (et toujours un nombre impair de fois) l'équation

$$5m=(10t+1)^2+2p^{4l+1}y^2,$$

» $t$ étant un entier quelconque, pair ou impair, positif, nul ou négatif, tandis que $y$ et $p$ sont impairs et positifs, de plus $p$ premier et » non diviseur de $y$. »

En d'autres termes, si du quintuple d'un nombre premier, de l'une ou de l'autre des deux formes

$$40\mu+7,\quad 40\mu+23,$$

on retranche, tant que faire se peut, les termes de la suite

$$1^2,\ 9^2,\ 11^2,\ 19^2,\ 21^2,\ldots,$$

que la formule

$$(10t+1)^2$$

fournit en y prenant $t=0$, $t=\pm 1$, $t=\pm 2,\ldots$, il y aura un nombre impair de restes susceptibles d'être mis sous la forme

$$2p^{4l+1}y^2;$$

$p$ etant un nombre premier non diviseur de $y$.

Il est bien évident que l'entier $y$ est impair. Quant à la forme linéaire du nombre premier $p$, nous remarquerons que, dans les conditions où nous nous sommes placés, l'équation

$$5m=(10t+1)^2+2p^{4l+1}y^2$$

entraîne ces deux congruences

$$p\equiv 1 \pmod{4}$$

et

$$p\equiv \pm 3 \pmod{5}.$$

Il s'ensuit que $p$ est de l'une des deux formes

$$20\nu+13,\quad 20\nu+17.$$

Nous nous bornerons aux exemples les plus simples en prenant d'abord $m=7$, $m=23$, $m=47$. Pour chacun de ces nombres, on trouve une seule équation canonique, savoir

$$5.7=1^2+2.17.1^2,$$

puis

$$5.23=9^2+2.17.1^2,$$

enfin

$$5.47=1^2+2.13.3^2.$$

Notre théorème se vérifie également pour $m=103$; mais on a alors

trois équations canoniques :

$$5.103 = 1^2 + 2.257.1^2,$$
$$5.103 = 11^2 + 2.197.1^2,$$
$$5.103 = 21^2 + 2.37.1^2.$$

*Théorème II.* — « Pour chaque nombre premier $m$, de l'une ou de » l'autre des deux formes $40\mu + 7$, $40\mu + 23$, on peut poser au » moins une fois (et toujours un nombre impair de fois) l'équation

$$5m = (10t + 3)^2 + 2p^{4l+1}y^2,$$

» $t$ étant un entier quelconque, pair ou impair, positif, nul ou négatif, » tandis que $y$ et $p$ sont impairs et positifs, de plus $p$ premier et non » diviseur de $y$. »

En d'autres termes, si du quintuple d'un nombre premier, de l'une ou de l'autre des deux formes

$$40\mu + 7, \quad 40\mu + 23,$$

on retranche, tant que faire se peut, les termes de la suite

$$3^2, \ 7^2, \ 13^2, \ 17^2, \ 23^2, \ldots,$$

que la formule

$$(10t + 3)^2$$

fournit en y prenant $t = 0$, $t = \pm 1$, $t = \pm 2$, etc., il y aura un nombre impair de restes susceptibles d'être mis sous la forme

$$2p^{4l+1}y^2,$$

$p$ étant un nombre premier, non diviseur de $y$.

Il est bien évident que l'entier $y$ est impair. Quant au nombre premier $p$, on trouve, comme pour le théorème I, qu'il doit être de l'une des deux formes

$$20\nu + 13, \quad 20\nu + 17.$$

Cette fois encore, nous nous bornerons aux exemples les plus

simples. Faisant d'abord $m = 7$, $m = 23$, $m = 47$, nous trouverons notre théorème confirmé par les équations canoniques respectives

$$5.7 = 3^2 + 2.13.1^2,$$

puis

$$5.23 = 3^2 + 2.53.1^2,$$

enfin

$$5.47 = 3^2 + 2.113.1^2.$$

Il l'est également pour $m = 103$; car on a alors les trois équations canoniques que voici :

$$5.103 = 7^2 + 2.233.1^2,$$
$$5.103 = 13^2 + 2.173.1^2,$$
$$5.103 = 17^2 + 2.113.1^2.$$

Nous ne voyons aucun intérêt à pousser plus loin ces vérifications numériques.

# THÉORÈMES GÉNÉRAUX

CONCERNANT

## LES COURBES GÉOMÉTRIQUES PLANES D'UN ORDRE QUELCONQUE;

**PAR M. E. DE JONQUIÈRES.**

---

I. *Définitions.* — Je dirai que des courbes géométriques planes du degré $n$ forment une *série,* quand elles ont toutes en commun $\frac{1}{2}n(n+3)-1$ conditions quelconques, c'est-à-dire quand elles satisfont toutes à autant de conditions, moins une, qu'il en faut pour déterminer une courbe de ce degré; et, si N désigne le nombre des courbes de cette série qui peuvent, en outre de ces conditions communes auxquelles elles sont assujetties, passer par un point quelconque donné, je dirai que la série est *d'indice* N.

Par exemple, des coniques qui passent toutes par deux mêmes points et touchent deux mêmes droites, forment une série d'indice 4, parce qu'on peut faire passer quatre de ces courbes par un point quelconque.

Ainsi encore, les cercles osculateurs d'une courbe géométrique du degré $m$ forment une série d'indice $\frac{3}{2}m(m-1)$, parce qu'il ne faut qu'une condition pour déterminer un cercle osculateur, et que, par un point donné, il passe $\frac{3}{2}m(m-1)$ de ces cercles, ainsi qu'on le verra ci-après (XVII).

Si les conditions communes aux courbes de la série sont simplement des points, auquel cas elles en ont, comme on sait, $\frac{1}{2}(n-1)(n-2)$ autres communs, en outre des $\frac{1}{2}n(n+3)-1$ dont il s'agit, N est égal à l'unité, et la série, qui est alors d'indice 1, prend le nom de *faisceau.*

II. Je rappellerai aussi les définitions et les propositions suivantes :

1° *L'axe harmonique* d'un point, par rapport à une courbe géométrique, est une ligne droite, lieu géométrique des centres harmoniques, relatifs à ce point, des points de rencontre d'une transversale quelconque issue de ce point avec la courbe (Cotes).

2° L'axe harmonique d'un point d'une courbe n'est autre chose que la tangente à la courbe en ce point.

L'axe harmonique d'un point ne passe par ce point que dans le cas où ce point appartient à la courbe.

3° La *courbe polaire* d'un point, par rapport à une courbe de degré $m$, est le lieu géométrique des points dont les axes harmoniques passent par ce point : elle est du degré $(m-1)$.

4° Les courbes polaires des différents points d'une droite passent toutes par $(m-1)^2$ points fixes, *pôles* de la droite.

L'un des pôles d'une droite ne peut être situé sur cette droite que si elle est une tangente de la courbe $C_m$; ce pôle est alors le point de contact.

5° La courbe enveloppe des axes harmoniques des points d'une droite, par rapport à une courbe du degré $m$, est une courbe de la *classe* $(m-1)$. [Chasles, *Cours professé à la Sorbonne* en 1856-1857.]

III. Théorème I. — *La courbe enveloppe des axes harmoniques d'un point* P, *par rapport aux courbes d'ordre $n$ d'une série d'indice* N, *est de la classe* N.

Il suffit de prouver qu'on ne peut mener que N axes harmoniques par un point quelconque, par exemple par le point P lui-même.

En effet, les seuls axes harmoniques du point P qui passent en P, sont (II, 2°) les tangentes en ce point aux courbes de la série qui y passent elles-mêmes. Or le nombre de ces courbes est N par hypothèse. Tel est donc aussi le nombre des tangentes, c'est-à-dire des axes harmoniques qui passent en P; ce qui démontre le théorème.

IV. Lemme. — *Toutes les courbes $C_n$ d'une série d'indice* N *peuvent être représentées analytiquement par une équation* $F(y,x)$ *du degré $n$, dont tous les coefficients sont des fonctions algébriques, entières et rationnelles d'une indéterminée* λ, *qui s'élève, dans l'un d'entre eux au*

*moins, au degré* N, *mais jamais à un degré supérieur, tandis que* $\frac{1}{2}n(n+3)-1$ *d'entre eux sont de certaines fonctions déterminées des paramètres des* $\frac{1}{2}n(n+3)-1$ *équations qui expriment les conditions auxquelles sont assujetties toutes les courbes de la série.*

En effet, pour toute valeur de $\lambda$, l'équation représente une courbe du degré $n$ satisfaisant aux conditions de la série; et, si l'on substitue à $x$ et $y$ les valeurs qui conviennent aux coordonnées d'un point quelconque donné $a$, on obtient une équation du degré N en $\lambda$ qui donne N valeurs de cette indéterminée et par conséquent N courbes distinctes passant sur le point $a$, ce qui est précisément le caractère de la série d'indice N que l'on considère.

Par exemple, si $N = 1$, c'est-à-dire si les courbes forment un faisceau, et que les équations de deux d'entre elles soient

$$y^n + axy^{n-1} + bx^n + \ldots + sy + tx + u = 0$$
$$y^n + a'xy^{n-1} + b'x^n + \ldots + s'y + t'x + u' = 0,$$

on sait que l'équation d'une courbe quelconque du faisceau sera ($\lambda$ représentant une indéterminée)

$$y^n(1+\lambda) + xy^{n-1}(a+\lambda a') + x^n(b+\lambda b') + \ldots + x(t+\lambda t') + (u+\lambda u') = 0,$$

qui satisfait aux conditions du Lemme.

V. Théorème II. — *Parmi les courbes* $C_n$ *d'une série d'indice* N, *il y en a* $2(n-1)$N *qui touchent une droite donnée* L.

En effet, la droite L coupe les courbes de la série en des points dont les abscisses sont, d'après le *Lemme*, les racines d'une équation du degré $n$ en $x$, dont certains coefficients, sinon tous, contiendront une indéterminée $\lambda$ au degré N, mais non pas à un degré supérieur.

A toute valeur de $\lambda$ qui rend égales deux racines de cette équation, il correspond une courbe $C_n$ qui touche la droite L. Or la condition d'égalité de deux racines s'exprime par une équation du degré $2(n-1)$

par rapport aux coefficients de l'équation en $x$ [*]. Donc cette équation de condition est du degré $2(n-1)\mathrm{N}$ en $\lambda$. Donc enfin il existe $2(n-1)\mathrm{N}$ courbes de la série qui touchent la droite L [**].

*Corollaire.* — On conclut sans difficulté du théorème précédent que :

Théorème III. — *Si par un point* P *on mène des tangentes aux courbes* $\mathrm{C}_n$ *d'une série d'indice* N, *le lieu des points de contact est une courbe de degré* $(2n-1)\mathrm{N}$, *qui passe* N fois *par le point* P.

On conclut ensuite de ce théorème que

*Si d'un point fixe on abaisse des normales sur les courbes d'une série d'ordre* $n$ *et d'indice* N, *leurs pieds sont situés sur une courbe du degré* $2n\mathrm{N}$;

Et en particulier que

*Le lieu des pieds des perpendiculaires abaissées d'un point fixe sur les tangentes d'une courbe géométrique du degré* $m$, *est une courbe du degré* $2m(m-1)$ *qui est douée, au point fixe, d'un point multiple de l'ordre* $m(m-1)$ [***].

J'ai démontré ce dernier théorème, par une voie différente, dans un article inséré au tome II (2e série) du *Journal de Mathématiques*.

VI. On peut aussi démontrer directement le théorème III, duquel le théorème II se déduit ensuite immédiatement.

Pour cela je prouverai d'abord que

---

[*] Voir, par exemple, la *Note sur l'élimination* qui se trouve dans l'appendice du *Traité* du Rév. G. Salmon *sur les courbes supérieures*, p. 296.

[**] Cette formule semble être en défaut quand, $n$ étant égal à 2, il y a plus d'une droite tangente parmi les conditions communes aux coniques de la série. Cette anomalie apparente sera expliquée ci-après (X).

[***] Cette courbe possède, à l'infini sur un cercle, deux autres points multiples, imaginaires, de l'ordre $m(m-1)$ (Chasles, *Comptes rendus*, t. LI, *Propriétés relatives au déplacement fini d'un corps, etc.*, § 24).

Théorème IV. — *Les courbes polaires d'un point* P *relatives aux courbes* $C_n$ *d'une série d'indice* N *forment elles-mêmes une série d'indice* N, *mais d'ordre* $(n-1)$.

Toutes ces courbes polaires sont du degré $(n-1)$; il ne faut plus qu'une seule condition pour déterminer chacune d'elles. Donc tout ce qu'il reste à prouver, c'est qu'il passe N de ces polaires, et pas davantage, par un point quelconque I.

En effet, une courbe polaire d'un point P est le lieu des points dont les axes harmoniques passent par ce point (II, 3°). Donc il passe par le point I autant de courbes polaires du point P, qu'il passe par le point P d'axes harmoniques du point I. Mais les axes harmoniques du point I enveloppent une courbe de la classe N (théor. I); donc il en passe N par le point P. Donc aussi il passe N courbes polaires du point P par le point I; ce qui démontre le théorème.

Je prouverai en second lieu que

Théorème V. — *Si à une courbe* $C_n$ *d'une série d'ordre* $m$ *et d'indice* N *il ne correspond qu'une seule courbe* $C_n$ *dans une autre série d'ordre* $n$ *et d'indice* N, *et réciproquement, le lieu des points d'intersection de deux courbes* $C_m$ *et* $C_n$ *correspondantes est du degré* $N(m+n)$.

Il faut prouver que le lieu cherché possède $N(m+n)$ points sur une droite quelconque S.

Soit $m$ un point variable de L : il passe par ce point N courbes $C_m$ donnant lieu à N groupes de $m$ points chacun sur L; appelons généralement $x$ les abscisses de ces points d'intersection. Aux N courbes $C_m$ il correspond par hypothèse, et une à une, N courbes $C_n$, lesquelles donnent lieu sur L à N groupes de $n$ points $m'$ chacun, correspondants groupe par groupe aux N premiers; appelons généralement $x'$ les abscisses de ces points $m'$.

A un point $m$ il correspond donc N groupes de points $m'$; et, réciproquement, à un point $m'$ il correspond N groupes de points $m$.

Donc les variables $x$ et $x'$ sont liées entre elles par une équation composée de N facteurs dont chacun est de la forme

$$A x^m x'^n + B x^m x'^{n-1} + C x^{m-1} x'^n + \ldots = 0.$$

car toute valeur de $x'$ donne N groupes de $m$ valeurs de $x$, et toute valeur de $x$ donne N groupes de $n$ valeurs de $x'$.

Pour tous les points de L qui appartiennent à la fois à deux courbes correspondantes $C_m$, $C_n$, on a $x = x'$. Or cette hypothèse réduit l'équation ci-dessus à une équation en $x$ seul composée de N facteurs chacun du degré $(m+n)$ et qui a par conséquent $N(m+n)$ racines. Tel est donc aussi le nombre des points de L qui appartiennent au lieu cherché. C. Q. F. D.

*Corollaire.* — Si les courbes de la première série sont les courbes polaires d'un point P par rapport à celles de la seconde, on a $m = (n-1)$; les courbes se correspondent une à une, et le lieu de leurs points d'intersection mutuels est, d'après ce qui précède, du degré $N(2n-1)$. Or un point d'intersection d'une $C_n$ et de sa polaire a pour axe harmonique une droite tangente à $C_n$ en ce point et qui passe par le point P. Donc le théorème III est démontré et par conséquent aussi le théorème II.

VII. Théorème VI. — *Le lieu des pôles d'une droite* L, *relatifs aux courbes* $C_n$ *d'une série d'indice* N, *est une courbe du degré* $2(n-1)N$, *c'est-à-dire dont le degré est égal au nombre des* $C_n$ *qui touchent une droite quelconque.*

Il suffit de prouver que le lieu cherché possède $2(n-1)N$ points sur une droite quelconque, par exemple sur la droite L elle-même.

En effet, les seuls pôles de L qui puissent exister sur cette droite sont (II, 4°) les points de contact des courbes de la série qui lui sont tangentes. Or le nombre de ces courbes est $2(n-1)N$ d'après le théorème II. Tel est donc aussi le nombre des points de contact, c'est-à-dire le nombre des pôles situés sur L.

VIII. Théorème VII. — *Le lieu des points qui ont même axe harmonique par rapport à une courbe fixe* $C_m$ *du degré* $m$, *et par rapport à l'une des courbes* $C_n$ *d'une série d'indice* N, *est une courbe du degré* $N(m+2n-3)$.

Il faut prouver que, sur une droite quelconque L, il existe $N(m+2n-3)$ points satisfaisant à la question.

Désignons par $x$ et $x'$ les abscisses de deux points variables $m$, $m'$ de L, dont la dépendance mutuelle va être expliquée.

Un point $m$ donne lieu à un seul axe harmonique X de ce point, relativement à la courbe fixe $C_m$; et, d'après le théorème VI, il existe, sur L, $2(n-1)N$ points $m'$, et pas davantage, qui ont cette même droite X pour axe harmonique relativement à certaines courbes de la série.

Réciproquement, un point $m'$ a pour axes harmoniques, relatifs aux $C_n$ de la série, toutes les tangentes à une courbe de la classe N (théorème I). Cette courbe a $N(m-1)$ tangentes communes avec la courbe enveloppe (II, 5°) des axes harmoniques des points de L par rapport à la $C_m$ fixe. Ainsi il existe $N(m-1)$ axes harmoniques du point $m'$, relatifs aux $C_n$, qui sont en même temps des axes harmoniques de certains points de L par rapport à la $C_m$ fixe, et ces points $m$ sont au nombre de $N(m-1)$. En d'autres termes, à un point $m'$ il correspond (en se renfermant dans les conditions de la question) $N(m-1)$ points $m$, tandis qu'à un point $m$ il correspond, comme on l'a dit plus haut, $2(n-1)N$ points $m'$.

Donc les abscisses $x$ et $x'$ de ces points sont liées entre elles par une équation de la forme

$$Ax^{N(m-1)}.x'^{2(n-1)N}+\ldots=0.$$

Si l'on y suppose $x=x'$, l'équation en $x$ seul aura pour racines les abscisses des points dont chacun a même axe harmonique dans la $C_m$ fixe et dans l'une des $C_n$. Or cette équation est du degré $N(m+2n-3)$ en $x$. Tel est donc aussi le nombre des points de L qui jouissent de la propriété énoncée; ce qui démontre le théorème.

Si $N=1$, les $C_n$ forment un faisceau, et l'on retrouve une proposition que M. Chasles a démontrée, d'une manière très-différente, dans ses *Cours de la Sorbonne*.

*Remarque.* — L'énoncé du théorème VII doit subir une légère modification, dans le cas où l'une des conditions auxquelles sont assujetties toutes les courbes de la série est de toucher la courbe fixe $C_m$, par rapport à laquelle on prend les axes harmoniques.

En effet, puisque chacune des $C_n$ touche cette courbe, chacun des points de la $C_m$ jouit de la propriété d'avoir le même axe harmonique par rapport à elle et par rapport à l'une des courbes de la série; de telle sorte que le lieu proprement dit se réduit alors, abstraction faite de cette $C_m$ qui en est une branche, à une courbe du degré $N(m+2n-3)-m$.

Cette remarque sera utile ci-après (XII).

IX. Théorème VIII. — *Le nombre des courbes $C_n$ d'une série d'indice N qui touchent une courbe fixe $C_m$ est* $Nm(m+2n-3)$.

Supposons qu'une $C_n$ touche la $C_m$ en $\alpha$. Ce point appartient à la courbe $C_{N(m+2n-3)}$ du théorème précédent. Car son axe harmonique, relatif à la $C_m$ ou à la $C_n$, indistinctement, est la tangente $\alpha t$ commune aux deux courbes. Le lieu $C_{N(m+2n-3)}$ coupe la courbe $C_m$ en $Nm(m+2n-3)$ points. L'un quelconque de ces points jouit de la propriété d'avoir le même axe harmonique dans la $C_m$ et dans l'une des courbes de la série. Mais le premier axe est tangent à $C_m$, puisque son pôle est sur $C_m$, et il passe par ce pôle. Donc (II, 4°) celle des $C_n$, relativement à laquelle il est aussi l'axe de ce pôle, est aussi tangente à $C_m$ en ce point.

Donc enfin il existe, en général, et sauf la diminution causée par l'existence de points multiples dans la courbe $C_m$, $Nm(m+2n-3)$ points de contact de la $C_m$ avec les courbes de la série.

*Remarque.* — Dans le cas où $N=1$, les $C_n$ forment un faisceau, et le théorème devient celui qui a été donné, dans les *Cours de la Sorbonne*, par M. Chasles, dont j'ai ici suivi le mode de démonstration.

X. Supposons que les conditions communes aux $C_n$ soient de toucher une courbe fixe $C_{m_1}$ et de passer par $\frac{1}{2}n(n+3)-2$ points. D'après la *remarque* du paragraphe précédent, N est alors égal à $m_1(m_1+2n-3)$. Donc, d'après le théorème VIII, le nombre des $C_n$ qui toucheront une seconde courbe fixe $C_m$ sera

$$m_1 m_2(m_1+2n-3)(m_2+2n-3).$$

Si les conditions communes consistent à toucher deux courbes fixes

$C_{m_1}$, $C_{m_2}$ et à passer par $\frac{1}{2}n(n+3)-3$ points, on aura, d'après ce qu'on vient de dire, $N = m_1 m_2 (m_1 + 2n - 3)(m_2 + 2n - 3)$. Donc le nombre des $C_n$ qui touchent une troisième courbe fixe $C_m$ est

$$m_1 m_2 m_3 (m_1 + 2n - 3)(m_2 + 2n - 3)(m_3 + 2n - 3).$$

En continuant ces raisonnements, on arrive au théorème suivant, qui n'est d'ailleurs qu'un cas particulier du théorème VIII, savoir :

Théorème IX. — *Si des courbes du degré $n$ doivent passer par $\frac{1}{2}n(n+3)-\mu$ points, et toucher $\mu$ courbes de degrés respectifs $m_1$, $m_2$, $m_3$, ..., $m_\mu$, le nombre des $C_n$ qui satisfont à la question est*

$$m_1 m_2 m_3 \ldots m_\mu (m_1 + 2n - 3)(m_2 + 2n - 3)(m_3 + 2n - 3) \ldots (m_\mu + 2n - 3).$$

XI. Cette formule a été donnée par M. Bischoff dans le *Journal de Crelle* (t. LVI), et déduite par ce géomètre de considérations très-différentes de celles qui précèdent.

Elle *paraît* être en défaut quand, $n$ étant égal à 2, c'est-à-dire quand les $C_n$ étant des coniques, il y a plus de deux droites tangentes parmi les conditions de la question. Ainsi elle donne 32 pour le nombre des coniques qui touchent cinq droites ; 8 pour celui des coniques qui en touchent trois et qui passent par deux points, etc.

Pour se rendre compte de cette singularité, il faut remarquer que des coniques, qui se trouvent en présence de trois droites qu'elles doivent toucher, prennent une dépendance mutuelle toute particulière, résultant de ce fait que les trois droites, qui joignent les sommets du triangle donné aux points de contact de chaque conique avec les côtés opposés, doivent passer par un même point. Le nombre des coniques qui satisfont à la question peut ainsi se trouver diminué, parce que plusieurs d'entre elles deviennent coïncidentes. Ainsi, quand des coniques circonscrites à un quadrilatère doivent toucher une droite, il y a généralement deux solutions. Mais si deux côtés opposés du quadrilatère deviennent infiniment petits, c'est-à-dire si les courbes doivent toucher deux droites fixes en deux points donnés, les points de contact

avec la troisième se confondent en un seul, et il semble ne plus y avoir qu'une seule conique tangente. On ne doit donc pas s'étonner que l'adjonction d'une quatrième et d'une cinquième droite tangente, en augmentant la dépendance mutuelle des coniques, fasse diminuer, dans une progression rapide, le nombre des solutions, en les identifiant les unes avec les autres.

La cause intime de cette exception, que présentent les courbes du *second degré*, me paraît d'ailleurs résider dans cette autre propriété singulière et caractéristique dont elles sont douées, d'avoir pour polaires réciproques des courbes du même degré qu'elles. Car il en résulte, dans toutes les questions où il entre des points ou des droites tangentes, que le nombre des solutions, au lieu de suivre une progression continue, comme cela a lieu pour les courbes d'un ordre plus élevé, au fur et à mesure qu'une tangente se substitue à un point dans les conditions données, il en résulte, dis-je, que ce nombre cesse de croître dès que celui des tangentes devient égal à celui des points, et diminue ensuite par une progression inverse de celle qu'il avait suivie d'abord. Par exemple, il y a douze coniques qui touchent une conique et une droite données et qui passent par trois points, et il y a pareillement, à cause de la polarité réciproque qui ramène ce second cas au premier, douze coniques touchant une conique et trois droites fixes et passant par un point. Mais sans doute ces douze coniques en représentent en réalité quarante-huit, qui sont superposées quatre par quatre; et de même dans toutes les autres questions du même genre.

XII. Supposons que, dans celle des formules du § X qui est relative à deux courbes tangentes, ces deux courbes se confondent en une seule $C_m$, la formule devient $m^2\,\overline{(m+2n-3)}^2$, et elle se rapporte au nombre des courbes du degré $n$ qui, passant par $\frac{1}{2}n(n+3)-2$ points, ont avec la $C_m$ un double contact.

Mais il faut faire subir à ce nombre une diminution dont je vais expliquer les causes.

En premier lieu, la courbe du théorème VII, lieu des points qui ont même axe harmonique par rapport à la $C_m$ et aux $C_n$, n'est plus que

du degré $m(m+2n-3)^2-m$, d'après la *remarque* du § VIII. Donc elle ne coupe la $C_m$ qu'en $m^2(m+2n-3)^2-m^2$ points, dont chacun est un point de tangence d'une $C_n$ ayant un double contact avec $C_m$.

Mais, en outre, il faut en déduire le nombre de fois que l'une des $C_n$ a un point double sur $C_m$; car l'axe harmonique d'un point double d'une courbe, par rapport à cette courbe, passe par ce point et y a une direction indéterminée; d'où il résulte que les deux axes harmoniques de chacun de ces points doubles situés sur $C_m$, par rapport à la $C_m$ et à la $C_n$ qui y possède ce point double, peuvent être regardés comme coïncidents, sans que cette $C_n$ ait un double contact proprement dit avec la $C_m$.

Or on sait que les points doubles d'un *système* de courbes du degré $n$, qui passent par $\frac{1}{2}n(n+3)-2$ points communs, sont situés sur une courbe du degré $3(n-1)$. Donc il y en a $3m(n-1)$ sur $C_n$.

D'après cela, la formule précédente se réduit à

$$m^2(m+2n-3)^2-m^2-3m(n-1).$$

Mais le nombre qu'elle exprime représente évidemment :

1° Le double du nombre des $C_n$ distinctes qui ont avec $C_m$ un *double contact* proprement dit;

2° Le triple du nombre des $C_n$ distinctes qui ont avec $C_m$ un contact du second ordre; car chacune d'elles en représente trois superposées et qui étaient distinctes dans le cas général pour lequel la formule a été établie.

Soient $x$ le nombre des $C_n$ qui ont un double contact bi-ponctuel, et $y$ celui des $C_n$ qui ont un double contact ordinaire; on aura donc

$$2y+3x=m^2(m+2n-3)^2-m^2-3m(n-1).$$

Or, d'après M. Bischoff, de Munich, dans l'article du *Journal de Crelle* déjà cité, on a

$$x=3m(m+n-3);$$

Donc le nombre des $C_n$ qui ont un double contact, proprement dit, avec $C_m$, est enfin

$$y = \frac{1}{2}\left[m^2(m+2n-3)^2 - m^2 - 3m(n-1) - 9m(m+n-3)\right]$$

ou

$$y = \frac{1}{2}m^2(m+2n-3)^2 - m(5m+6n-15):$$

ce qui est aussi la formule donnée, pour ce cas, par M. Bischoff.

Les mêmes considérations s'appliquent naturellement à la recherche du nombre des tangentes doubles des courbes géométriques ; et ce nombre résulte directement de la formule précédente, en y faisant $n=1$ ; mais j'aurai occasion de revenir plus loin (XVIII) sur cette intéressante question.

XIII. Théorème X. — *La courbe enveloppe des cordes communes à une courbe fixe $C_m$ du degré $m$, et aux courbes $C_n$ d'une série d'ordre $n$ et d'indice $N$, est de la classe $\frac{1}{2}m(m-1)(2n-1)N$.*

Il faut prouver que, par un point quelconque O, il passe $\frac{1}{2}m(m-1)(2n-1)N$ droites, sur chacune desquelles deux points *distincts*, appartenant à la $C_m$, coïncident avec deux points d'une même courbe $C_n$.

Soit $x$ la distance à une origine fixe P, prise sur une droite arbitraire L, d'un point variable sur cette droite. Par chaque point dont l'abscisse est $x$, il passe, par hypothèse, N courbes de la série des $C_n$, et chacune de ces $C_n$ coupe la $C_m$ fixe en $mn$ points. Projetant tous ces points d'intersection sur L, à partir du point O, et appelant $y$ les abscisses de ces points projetés, on aura, sur L, N systèmes de $mn$ points chacun, correspondants à la fois à l'abscisse $x$. Je dis N systèmes de $mn$ points, et non pas un système de $Nmn$ points, parce que la nature même de la question ne permet pas de joindre un point d'intersection de la $C_m$ provenant d'une courbe $C_n$ avec l'un des points d'intersection de cette $C_m$ provenant d'une autre

$C_n$ [*], pour en faire l'une des cordes dont on cherche l'enveloppe; mais, au contraire, les deux points d'intersection doivent provenir d'une même $C_n$.

En d'autres termes, l'équation en $y$, dont les racines pourront représenter les abscisses de tous les $Nmn$ points projetés, ne sera pas une équation générale du degré $Nmn$, mais bien le produit de N équations distinctes, chacune du degré $mn$ seulement.

Réciproquement, à une abscisse $y$ d'un point Y de L, il correspond, sur la droite OY, $m$ points d'intersection de la $C_m$ fixe par cette droite; et, pour chacun de ces $m$ points, N courbes appartenant à la série des $C_n$; donc $m$N valeurs de $x$.

Ainsi l'équation qui exprime la dépendance mutuelle des $y$ et des $x$, se compose du produit de N équations, dans chacune desquelles $y$ entre au degré $mn$, tandis que ses coefficients contiennent $x$ au degré $m$N.

Pour qu'une des cordes communes à la $C_m$ et à l'une des $C_n$ passe par le point O, il faut, non plus que l'équation générale ait deux racines égales (ainsi que je l'ai fait remarquer plus haut), mais simplement que l'une des N équations, dans lesquelles elle se décompose en facteurs, ait deux racines égales.

Or, chacune de ces équations composantes étant du degré $mn$ en $y$, l'équation de condition qui exprime l'égalité de deux racines sera du degré $2(mn-1)$ par rapport à ses coefficients; donc elle sera du degré $2m\mathrm{N}(mn-1)$ en $x$. C'est-à-dire que cette circonstance de l'égalité de deux racines $y$ égales entre elles se présentera $2m\mathrm{N}(mn-1)$ fois pour l'infinité des valeurs de $x$. Chacune de ces racines égales correspond à une valeur de $x$, laquelle détermine N courbes $C_n$. Mais, parmi ces N courbes, il n'y en a, en général, qu'une seule qui satisfasse à la question. Car dire que deux racines en $y$ sont égales, c'est dire que deux points d'intersection $a$, $b$, de la $C_m$ avec une $C_n$ sont en ligne droite avec le point O, et s'il arrive, comme ici, que ces deux points sont situés à la fois sur une même $C_n$ passant par le point dont l'abscisse est $x$, les $\mathrm{N}-1$ autres ne jouiront pas de cette propriété.

---

[*] Le sens précis de cette réflexion sera mieux compris dans un instant.

Actuellement, il y a deux remarques à faire sur la formule précédente $2mN(mn-1)$; c'est d'abord qu'elle exprime, non-seulement le nombre de fois que deux points d'intersection distincts de la $C_m$ et d'une $C_n$ sont en ligne droite avec le point O, mais aussi le nombre de fois que ces deux points sont coïncidents, c'est-à-dire le nombre des contacts de la $C_m$ fixe avec les courbes de la série. Or le nombre de ces contacts est, d'après le théorème VIII, $Nm(m+2n-3)$. Donc la formule devient, en premier lieu,

$$2mN(mn-1)-Nm(m+2n-3)=m(m-1)(2n-1)N.$$

Mais je dis, en outre, qu'il ne faut prendre que la moitié de ce nombre, parce que l'analyse précédente, basée sur la théorie des racines égales, conduit nécessairement ici à considérer deux fois la même corde, et que, si $a$ et $b$ sont deux points d'intersection de la $C_m$ et d'une $C_n$, situées en ligne droite avec le point O, le calcul donne aussi bien la corde $ab$ que la corde $ba$ [*], ce qui double le nombre des solutions réellement distinctes. Donc enfin le nombre des cordes communes qui passent par le point O est $\frac{1}{2}m(m-1)(2n-1)N$; ce qui démontre le théorème.

XIV. Si les courbes de la série forment un faisceau, $N=1$ et le théorème prend cet énoncé :

THÉORÈME XI. — *Les cordes communes à une $C_m$ fixe et à un*

---

[*] Il en est ici, comme dans le cas où il s'agit d'évaluer les distances mutuelles de $m$ points. Le nombre de ces distances est $m(m-1)$, puisque chacun des $m$ points doit être joint aux $(m-1)$ autres. Mais, comme chacune se répète deux fois, le nombre des distances réellement distinctes n'est que $\frac{1}{2}m(m-1)$.

Le même fait se présente, quand on applique la théorie des racines égales à la recherche du nombre des tangentes qu'on peut mener d'un point à une courbe du degré $m$, ce qui est extrêmement simple. L'équation de condition, à laquelle on arrive par des raisonnements analogues à ceux qui précèdent, est du degré $2m(m-1)$. Mais, comme chaque tangente se trouve répétée deux fois, le nombre des tangentes réellement distinctes qu'on peut mener à la courbe n'est que la moitié du précédent, c'est-à-dire $m(m-1)$, comme on le démontre de beaucoup d'autres manières.

*faisceau de* $C_n$ *enveloppent une courbe de la classe* $\frac{1}{2}m(m-1)(2n-1)$.

XV. Si les courbes de la série passent toutes par un même point $a$, et que ce point soit situé sur la $C_m$ fixe, la classe de l'enveloppe est diminuée de $(m-1)N$; et si elles passent par $p$ points communs situés sur la $C_m$, cette classe est diminuée de $p(m-1)N$.

Car la droite $Oa$, par exemple, coupe $C_m$ en $(m-1)$ autres points $b$, $c$, $d$, etc. Il y a N courbes de la série qui passent en $a$ et $b$; N qui passent en $a$ et $c$; etc. Donc $Oa$ est $N(m-1)$ fois une corde commune à la $C_m$ et aux $C_n$; et ceci a lieu quel que soit le point O. Donc le point $a$ est un point isolé de la courbe enveloppe et, qui plus est, un point multiple de la classe $N(m-1)$; de sorte que la classe de la courbe enveloppe proprement dite, et en faisant abstraction de ce point, se trouve abaissée de $N(m-1)$ unités.

On en conclut en particulier que

*Les coniques d'un faisceau, qui passent par deux points d'une conique fixe, la coupent encore suivant des cordes concourantes en un même point ;*

Que

*Les cubiques d'un faisceau, qui passent par sept points d'une cubique fixe, interceptent dans cette courbe des cordes concourantes en un même point ;*

Que

*Les coniques d'un faisceau, qui passent par quatre points d'une courbe du troisième ordre, la coupent encore suivant des droites qui passent toutes par un point fixe ;*

Que

*Les coniques d'une série, qui touchent toutes une droite fixe et qui passent par trois points, dont deux sont situés sur une conique donnée, coupent cette courbe suivant des cordes qui enveloppent une autre conique ;*

Ou que

*Les coniques d'un faisceau, qui ont toutes un point commun avec une*

*conique fixe, la coupent suivant des cordes qui enveloppent une autre conique;* théorème cité et utilisé par M. Chasles dans sa *Note sur la construction de la courbe du troisième ordre,* insérée dans le tome XXXVII des *Comptes rendus de l'Académie des Sciences*, page 276.

Etc., etc.

XVI. Dans le cas où la courbe fixe $C_m$, qui se trouve en présence de la série des $C_n$, est douée, en un point P, d'un point multiple de l'ordre $(m-1)$, on peut arriver à la formule générale du théorème X par des considérations de pure géométrie qui, indépendamment de l'espèce de confirmation qu'elles donnent à cette formule, me semblent assez intéressantes pour trouver place ici.

Pour trouver, dans ce cas, la classe de l'enveloppe des cordes communes, il suffit de prouver que, par un point quelconque, le point P par exemple, il passe $\frac{1}{2}m(m-1)(2n-1)$N cordes.

Or il est évident que les seules courbes $C_n$ qui puissent alors donner lieu à des cordes passant en P, sont celles qui passent elles-mêmes par ce point, puisque, par la nature du point multiple, toute droite qui y passe ne peut plus rencontrer la courbe qu'en un seul point.

Ces courbes sont en nombre N, par hypothèse. Chacune d'elles coupe $C_m$ en $mn-(m-1)$ points, autres que le point multiple P; et chacun de ces points d'intersection donne lieu à $(m-1)$ cordes, si on le suppose joint aux $(m-1)$ points d'intersection qui sont confondus en un seul au point P. On obtient donc ainsi d'abord $(m-1)[mn-(m-1)]$ cordes aboutissant en P.

En outre, les $(m-1)$ points confondus en P, ou, si l'on veut, qui y sont infiniment voisins l'un de l'autre, donnent lieu à $\frac{1}{2}(m-1)(m-2)$ distances mutuelles ou cordes aboutissant à ce point. On aura donc un total de

$$(m-1)\left[mn-(m-1)+\frac{1}{2}(m-2)\right]=\frac{1}{2}m(m-1)(2n-1);$$

et enfin, puisqu'il y a N courbes $C_n$ qui passent en P, et dont chacune produit le même résultat, le nombre total des cordes communes issues du point P est $\frac{1}{2}m(m-1)(2n-1)$N. C. Q. F. D.

XVII. Une des applications les plus intéressantes qu'on puisse faire du théorème XI, relatif à la courbe enveloppe des cordes communes à une $C_m$ fixe et à un faisceau de $C_n$, est celle qui a pour objet la recherche du nombre des *tangentes doubles* que possède une courbe du degré $m$. La solution qu'il fournit de cette question, qui a longtemps présenté des difficultés, ne le cède en élégance et en simplicité à aucune autre.

Je commencerai par rappeler, sous forme de *Lemme*, la proposition suivante qui est due à M. O. Hesse.

LEMME. — *Une courbe géométrique du degré $m$ a, en général, $3m(m-2)$ points d'inflexion.*

Cette proposition peut elle-même se prouver, en quelques mots, de la manière suivante :

Supposons qu'un point $a$ se meuve sur une droite quelconque L. Ses courbes polaires successives, par rapport à la courbe $C_m$, forment un faisceau de l'ordre $(m-1)$ (II, 4°). D'après le théorème VIII, le nombre des courbes de ce faisceau qui touchent la $C_m$ est $m(3m-5)$. Or, quand une courbe polaire du point $a$ touche la $C_m$ en $t$, la droite $at$, au lieu d'être, comme dans le cas où le point $t$ est un point d'intersection des deux courbes, simplement tangente à $C_m$ en $t$, y touche cette courbe suivant deux éléments consécutifs, c'est-à-dire est tangente en un point d'inflexion, à moins pourtant que le point $a$ n'appartienne lui-même à la $C_m$. Car, dans ce cas, sa courbe polaire touche C en $a$, sans que la tangente commune de ces deux courbes soit, en général, une tangente d'inflexion. Or, cette seconde circonstance se présente pour chacun des $m$ points d'intersection de $C_m$ par L, c'est-à-dire $m$ fois seulement. Donc le nombre des points $a$, dont chacun est le point d'intersection de L par une tangente d'inflexion est seulement

$$m(3m-5)-m=3m(m-2). \; [*] \qquad \text{C. Q. F. D.}$$

[*] Sans rien changer à l'enchaînement des raisonnements qui précèdent, si l'on suppose que, de chaque position du point $a$, on abaisse des normales sur la $C_m$, leurs pieds sont situés sur une courbe du degré $m$ et toutes ces courbes forment un faisceau. Quand une de ces courbes touche la $C_m$, le point de L, duquel elle dérive, est un centre de courbure. On en conclut donc immédiatement que *la développée d'une courbe géométrique du degré $m$ est une courbe du degré $3m(m-1)$ dont la classe est $m^2$.*

Ceci posé, il est très-facile de prouver que

Théorème XI. — *Une courbe géométrique du degré $m$ a, en général, $\frac{1}{2}m(m-2)(m^2-9)$ tangentes doubles.*

Supposons, comme précédemment, qu'un point $a$ se meuve sur une droite L, et qu'à chaque instant on joigne ce point par des droites $at$, $at'$, ..., aux $m(m-1)$ points d'intersection de la $C_m$ par la courbe polaire du point $a$.

Il arrivera que deux points d'intersection $t, t'$ seront en ligne droite avec le point $a$, dans les trois circonstances suivantes, savoir :

1° Quand la droite $att'$ sera une tangente double ; et alors les deux points $t$, $t'$ sont distincts et situés l'un et l'autre hors de L ;

2° Quand la droite $att'$ sera une tangente d'inflexion ; et alors les deux points $t, t'$ coïncident en dehors de L (voir le *Lemme*) ;

3° Quand le point $a$ sera un point d'intersection de la $C_m$ par L ; car la courbe polaire passant aussi par ce point, il est lui-même l'un des points $t$ ; de sorte que la droite $at'$ qui le joindra à l'un quelconque $t'$ des $m(m-1)-1$ autres points d'intersection de la $C_m$ par la courbe polaire, contiendra aussi deux points d'intersection $t$. $t'$ de ces deux courbes.

Or le second cas se présente $3m(m-2)$ fois, et le troisième se présente $m[m(m-1)-1]$ fois. Donc si l'on détermine le nombre total des fois que deux points $t$, $t'$ sont en ligne droite avec le point $a$, d'où ils dérivent, il suffira d'en retrancher

$$3m(m-2)+m[m(m-1)-1]=\frac{1}{2}m(2m^2+4m-14),$$

pour avoir précisément le nombre des tangentes doubles, proprement dites, de la courbe proposée.

Pour cela, remarquons que, à un point $a$ de L dont l'abscisse est $x$, il correspond $m(m-1)$ points d'intersection de la $C_m$ par la polaire de ce point : donc

$$\frac{1}{2}m(m-1)[m(m-1)-1]=\frac{1}{2}m(m^3-2m^2+1)$$

cordes distinctes joignant deux à deux ces points d'intersection. Cha-

cune de ces cordes coupe L en un point, dont l'abscisse sera désignée par $x'$ ; et, ce qu'il faut savoir, c'est combien de fois il arrive que les valeurs de $x$ et de $x'$ sont les mêmes.

On vient de voir que, à une valeur de $x$, il correspond

$$\frac{1}{2}m(m^3 - 2m^2 + 1)$$

valeurs de $x'$. Mais, à une valeur de $x'$, il correspond

$$\frac{1}{2}m(m-1)(2m-3) = \frac{1}{2}m(2m^2 - 5m + 3)$$

valeurs de $x$, parce que, d'après le théorème XI, il passe précisément ce nombre de cordes, communes à la $C_m$ et au faisceau des courbes polaires, par le point dont l'abscisse est $x'$, et que généralement chacune de ces cordes provient d'une courbe polaire particulière, c'est-à-dire qu'une courbe ne donne lieu, en général, qu'à une seule corde passant en un point donné.

Donc l'équation qui exprime la dépendance mutuelle des abscisses $x$ et $x'$ est de la forme

$$A x^{\frac{1}{2}m(2m^2 - 5m + 3)} . x'^{\frac{1}{2}m(m^3 - 2m^2 + 1)} + \ldots = 0.$$

Si l'on y suppose $x = x'$, on obtient une équation en $x$ seul, dont le degré est $\frac{1}{2}m(m^3 - 5m + 4)$; ce qui prouve que tel est aussi le nombre de fois que se présente la coïncidence des deux points dont les abscisses respectives sont $x$ et $x'$. Si l'on retranche de ce nombre celui qui est écrit plus haut, il vient, pour le nombre des tangentes doubles,

$$\frac{1}{2}m(m^3 - 5m + 4) - \frac{1}{2}m(2m^2 + 4m - 14) = \frac{1}{2}m(m-2)(m^2-9).$$

C. Q. F. D.

*Autrement.* — Le théorème qui précède peut aussi se conclure très-aisément de la formule générale du § X, relative à deux courbes. Si l'on y suppose que les deux courbes fixes soient du degré $m$ et que $n = 1$,

on en conclut d'abord qu'il y a $m^2(m-1)^2$ droites touchant deux courbes de degré $m$. Si les deux courbes sont égales, on pourra les amener, en déplaçant l'une d'elles, à se confondre en une seule. Considérons les deux courbes un instant avant que la coïncidence ait lieu. En chacun de leurs $m^2$ points d'intersection il y a deux tangentes distinctes, une pour chaque courbe; au moment où la coïncidence s'établit, ces deux tangentes n'en font plus qu'une seule, qui est une tangente simple de la courbe $C_m$, quoiqu'elle représente une tangente aux deux courbes superposées, c'est-à-dire une tangente double. Il faut donc d'abord déduire $m^2$ du nombre précédent. En outre, chaque tangente d'inflexion représente trois tangentes doubles superposées qui, n'étant pas des tangentes doubles proprement dites, doivent être retranchées aussi du nombre primitivement trouvé. On a donc enfin

$$m^2(m-1)^2 - 9m - (m-2) - m^2 = m(m-2)(m^2-9),$$

nombre dont il faut prendre la moitié, parce que chaque tangente double s'y trouve répétée deux fois, d'après la manière même dont il a été obtenu; ce qui démontre le théorème.

*Remarque.* — La formule précédente convient au cas où la $C_m$ est *générale* dans son degré. Si cette courbe a des points doubles ou de rebroussement, le nombre des tangentes doubles en est diminué, et l'on prouve très-aisément que, si D et D' sont, respectivement, les nombres de ces points singuliers, la formule devient

$$\frac{1}{2}m(m-2)(m^2-9) - (2D+3D')(m^2-m-6)$$
$$- 2D(D-1) - \frac{9}{2}D'(D'-1) - 3DD'.$$

Mais ce n'est pas ici le lieu d'entrer dans ces détails.

XVIII. Pour donner une autre application du théorème XI, je vais démontrer deux propriétés générales des courbes géométriques.

THÉORÈME XII. — *Les tangentes à une courbe géométrique $C_m$, menées aux points où cette courbe est rencontrée par une transversale qui pivote autour d'un point fixe S, se coupent, deux à deux, sur une courbe dont le degré est* $\frac{1}{2}m(m-1)(2m-3)$.

Il faut prouver que le lieu cherché possède $\frac{1}{2} m (m-1)(2m-3)$ points sur une droite quelconque L.

Or, si un point se meut sur L, les points de contact des tangentes à $C_m$, issues de ce point, sont, à chaque instant, sur la $C_{m-1}$, première courbe polaire de ce point par rapport à la $C_m$. Toutes les polaires forment un *faisceau* de l'ordre $(m-1)$. Donc leurs cordes communes avec $C_m$ enveloppent une courbe de la classe $\frac{1}{2} m(m-1)(2m-3)$ (théorème XI). Donc il passe précisément ce nombre de cordes communes par le point S. Or, pour chacune de ces cordes, il y a sur L un point de concours de deux tangentes menées à $C_m$ en deux points de rencontre d'une même transversale. Donc le théorème est démontré.

Cette démonstration se déduit aussi, avec beaucoup de facilité, de la théorie des racines égales. Mais ces détails seraient ici superflus.

*Corollaire.* — Si la droite L est à l'infini, les tangentes qu'on considère sont parallèles dans chaque couple, et l'on a ce théorème qui a été énoncé, sans démonstration, par M. Steiner dans un *Mémoire sur les Courbes algébriques*, dont M. Woepcke a donné une traduction dans le tome XVIII du *Journal de Mathématiques* (*voir* page 348, en note, au bas de la page) :

Théorème XIII. — *La courbe enveloppe des cordes qui joignent, deux à deux, les points de contact des tangentes d'une* $C_m$ *parallèles entre elles, est de la classe* $\frac{1}{2} m(m-1)(2m-3)$.

XIX. Voici encore une propriété nouvelle des courbes géométriques qui se déduit directement du théorème X.

Théorème XIV. — *Les normales à une* $C_m$, *menées aux points où cette courbe est rencontrée par une transversale qui pivote autour d'un point* S, *se coupent, deux à deux, sur une courbe du degré* $\frac{1}{2} m(m-1)(2m-1)$.

Il faut prouver que le lieu cherché possède $\frac{1}{2} m(m-1)(2m-1)$ points sur une droite quelconque L.

Supposons que, de chaque point de L, on abaisse $m^2$ normales sur

$C_m$. D'après un théorème démontré par M. Steiner, dans le tome XX du *Journal de Mathématiques*, page 36, les pieds de ces normales sont, à chaque instant, situés sur une courbe du degré $m$, et toutes ces courbes passent par $m^2$ points communs, c'est-à-dire forment un faisceau. Le lieu cherché possède, sur L, autant de points que ce faisceau et la $C_m$ fixe possèdent de cordes communes passant en S. Or ce nombre est $\frac{1}{2}m(m-1)(2m-1)$, d'après le théorème XI. Donc le théorème est démontré. On le déduit aussi, sans difficulté, de la théorie des racines égales.

Si l'on mène, par le point S, des parallèles aux $m$ asymptotes de la courbe $C_m$, et ensuite des normales à cette courbe en tous les points où ces parallèles la rencontrent à distance finie, on a d'abord les directions de $m(m-1)$ asymptotes de la courbe dont il s'agit. Il reste à déterminer celles des

$$\frac{1}{2}m(m-1)(2m-1) - m(m-1) = \frac{1}{2}m(m-1)(2m-3) \text{ autres.}$$

Et il est facile de voir que ce sont précisément les normales à la $C_m$ aux points de contact des tangentes parallèles dont il s'agit dans le théorème XIII, et dont les cordes de contact passent par le point S.

Etc.

Je terminerai ce Mémoire en faisant remarquer que les théorèmes XII et XIV sont susceptibles d'être généralisés ainsi qu'il suit :

Théorème XV. — *Étant données deux courbes fixes planes, l'une du degré* $m$ *et l'autre de la classe* $m'$; *si une tangente roule sur celle-ci, et que, par les points où elle rencontre la* $C_m$, *on mène à cette courbe ses tangentes et ses normales en ces points d'intersection, les tangentes se couperont, deux à deux, sur une courbe du degré* $\frac{1}{2}mm'(m-1)(2m-3)$, *et les normales se couperont, deux à deux, sur une courbe du degré* $\frac{1}{2}mm'(m-1)(2m-1)$.

Ces deux propositions se démontrent de la même manière que celles dont elles sont une simple extension.

## SUR LA FORME

## $x^2 + 3y^2 + 4z^2 + 12t^2$ ;

PAR M. J. LIOUVILLE.

Il est évident que la forme

$$x^2 + 3y^2 + 4z^2 + 12t^2$$

ne peut représenter aucun nombre impairement pair, attendu qu'on ne peut pas rendre le binôme $x^2 + 3y^2$ divisible par 2, sans le rendre en même temps divisible par 4. Mais je dis que pour tout nombre $m$, soit impair, soit multiple de 4 (c'est-à-dire de la forme $2^{2+\alpha} n$, $n$ étant impair et $\alpha$ égal à 0, 1, 2, etc.), une telle représentation existe, en sorte que l'on a, en nombres entiers,

$$m = x^2 + 3y^2 + 4z^2 + 12t^2.$$

C'est ce qu'on vérifie aisément pour les petits nombres 1, 3, 4, 5, 7, 8, etc.; mais il faut donner une démonstration générale.

Comme la forme

$$x^2 + 3y^2 + 4z^2 + 12t^2$$

est une de celles qui se reproduisent par la multiplication, il suffira de considérer : 1° le cas de $m$ premier impair, 2° le cas de $m = 2^{2+\alpha}$.

Or quand $m$ est un nombre premier $4\mu + 1$, on peut poser, en nombres entiers,

$$m = a^2 + 4b^2;$$

il suffira donc alors de faire $x = a$, $y = 0$, $z = b$, $t = 0$.

Quant aux nombres premiers $m$ de la forme $4\mu + 3$, on peut toujours poser pour eux l'équation

$$m = u^2 + v^2 + 3w^2,$$

qui convient évidemment au nombre 3, et qui a lieu aussi, comme Dirichlet l'a prouvé (cahier de juin 1859, p. 237-240), pour tout entier impair non multiple de 3. Mais quand $m$ est de la forme $4\mu + 3$, une telle équation ne peut exister qu'avec des valeurs paires de $u$ et $v$. On peut donc remplacer $v$ par $2s$ et écrire

$$m = u^2 + 3w^2 + 4s^2,$$

ce qui rentre dans notre équation générale

$$m = x^2 + 3y^2 + 4z^2 + 12t^2,$$

en faisant $x = u$, $y = w$, $z = s$, $t = 0$.

Restent les entiers contenus dans l'expression

$$2^{2+\alpha},$$

que l'on peut remplacer par l'une ou l'autre des deux que voici :

$$4.4^\beta, \quad 8.4^\beta,$$

suivant que $\alpha$ est pair ou impair. Or 4 et 8 sont représentés par la forme

$$x^2 + 3y^2 + 4z^2 + 3t^2,$$

en prenant $x = 0$, $y = 0$, $z = 1$, $t = 0$, puis $x = 1$, $y = 1$, $z = 1$, $t = 0$. D'ailleurs en doublant les valeurs de $x$, $y$, $z$, $t$, on rend la valeur de cette forme quatre fois plus grande. On passera ainsi de 4 à $4.4$, $4.4^2, \ldots, 4.4^\beta$ et de 8 à $8.4$, $8.4^2, \ldots, 8.4^\beta$. Notre démonstration est donc complète.

# ÉTUDE

SUR LES

# TRANSFORMATIONS HOMOGRAPHIQUES PLANES;

PAR M. F. LUCAS,

Ingenieur des Ponts et Chaussées, à Nice.

---

## § I. — *Définitions et notations.*

**1.** Lorsqu'on transforme une figure, par voie homographique, il y a généralement des points que la transformation ne déplace pas et qu'on peut, pour cette raison, appeler *points doubles*.

Deux points doubles étant réunis par une droite, cette ligne n'est pas déplacée par la transformation, et l'on est ainsi conduit à considérer des *droites doubles*.

Soient :

$m$ le nombre des points doubles;
$n$ celui des droites doubles.

Comme les points doubles résultent des intersections mutuelles des droites doubles, on a

$$(1) \qquad m = \frac{n(n-1)}{2},$$

et comme les droites doubles résultent de la jonction des points doubles pris deux à deux, on a

$$(2) \qquad n = \frac{m(m-1)}{2}.$$

Des équations (1) et (2), on tire

$$m = n = 3.$$

Il y a donc trois points doubles, parmi lesquels peut se trouver un couple de points imaginaires, et trois droites doubles qui peuvent présenter un couple de droites imaginaires.

Dans tous les cas, nous appellerons *triangle invariable* la figure formée par les points et les droites doubles, tant réels qu'imaginaires.

**2.** Étant définie, soit par des données géométriques, soit au moyen d'équations, une transformation homographique en vertu de laquelle on passe d'un *premier* à un *second* système de figures, ou réciproquement, une figure F du plan, considérée tour à tour, comme appartenant à chacun des deux systèmes, donnera naissance à deux homologues que nous désignerons respectivement par F′ et F″.

On voit que la transition de F à F′ se fait de la même manière que celle de F″ à F, que les trois figures F, F′, F″ sont deux à deux homographiques entre elles et que le triangle invariable est le même dans les trois systèmes correspondants (F, F′), (F′, F″), (F″, F).

**3.** Un point $m$ du plan donne naissance à deux homologues $m'$, $m''$, que l'on peut réunir par une droite M.

Cette droite $m$ donne naissance à deux homologues M′ et M″ qui se coupent en $m$.

Le point $m$ et la droite M ont donc entre eux une dépendance qui permet de passer du point à la droite ou de la droite au point, sans ambiguïté et d'une façon fort simple. Nous leur donnerons les noms de *foyer* et *directrice*.

## § II. — *Corrélation des points du plan et des coniques circonscrites au triangle invariable.*

**4.** Supposons que la droite M tourne autour d'un point $a$, M′ et M″ pivoteront respectivement autour de $a'$ et de $a''$, et leur intersection $m$, foyer de M, décrira une conique passant par $a'$ et $a''$ (*Géométrie supérieure*, n° 543) et aussi par les trois points doubles; en sorte que cette conique est déterminée par cinq points donnés. On voit par là comment un point $a$ détermine une conique $C_a$ circonscrite au triangle invariable.

On reconnaît aisément que les homologues $(C_a)'$ et $(C_a)''$ de la co-

nique $C_a$ se coupent au point $a$; donc une conique circonscrite au triangle invariable correspond toujours à un point du plan par la liaison précédemment définie; cette correspondance est simple et sans ambiguïté.

Pour exprimer cette correspondance, nous dirons que le point et la conique sont *conjugués*.

5. Remarquons en passant que les coniques $(C_a)'$ et $(C_a)''$, homographiques entre elles, sont respectivement engendrées par les homologues $m'$ et $m''$ du point $m$; or ces deux points sont situés sur la droite M qui pivote autour de l'intersection $a$ des deux coniques. De là ce théorème :

*Quand deux coniques homographiques sont circonscrites au triangle invariable de la transformation, chaque couple de points homologues, pris sur ces courbes, est en ligne droite avec le quatrième point d'intersection des deux coniques.*

6. Faisons mouvoir le point $a$ sur une droite X, la conique conjuguée $C_a$ de ce point pivotera, en se déformant, autour des sommets du triangle invariable et en outre autour du foyer $x$ de la droite X.

En effet, pour une position quelconque du point $a$ sur X, la droite pivotante M, qui tourne autour de $a$ et dont le foyer $m$ engendre $C_a$, coïncidera à un moment donné avec la droite X, et par conséquent $C_a$ passera par $x$. Par conséquent :

*Lorsqu'un point décrit une droite, sa conique conjuguée pivote autour d'un point, foyer de cette droite.*

Réciproquement le faisceau des coniques circonscrites au triangle invariable et passant par le point $x$ pourra être regardé comme l'ensemble des coniques conjuguées des différents points de la directrice X de ce point. Donc

*Lorsqu'une conique circonscrite au triangle invariable pivote autour d'un point, le point conjugué de cette conique engendre une droite directrice du pivot.*

7. Considérons maintenant le faisceau de coniques circonscrites au

triangle invariable déterminé par le foyer $x$ ou par la directrice X, et prenons relativement à ces coniques les polaires d'un point quelconque du plan. Toutes ces polaires passeront par un même point (*Géométrie supérieure*, n° 478, étendu aux coniques) et correspondront respectivement, sans ambiguïté, aux différents points de la droite X; elles formeront donc un faisceau en correspondance anharmonique avec la division conçue sur X. On peut dire par conséquent que :

*Les différents points d'une droite forment une série homographique avec la série de leurs coniques conjuguées.*

8. L'ensemble des observations que nous venons d'exposer dans ce paragraphe, nous conduit à énoncer le théorème suivant, qui résume tout ce qui précède :

*La correspondance entre les points et leurs coniques conjuguées présente tous les caractères essentiels de la correspondance dite corrélative.*

## § III. — *Nouvelle méthode de transformation des figures.*

9. De même que la correspondance corrélative des points et des droites conduit à une méthode de transformation des figures, de même la correspondance corrélative des points et des coniques conduit à une méthode de transformation, dont nous allons nous occuper.

Que le point $a$ se meuve suivant une loi continue quelconque, de manière à décrire une courbe $\Sigma$, et la conique conjuguée $C_a$ pivotera, en changeant de forme, autour des sommets du triangle invariable, de manière à envelopper une courbe $\Sigma_1$ correspondante à $\Sigma$.

Au lieu de définir la génération de $\Sigma_1$ par ses tangentes, on peut en définir une génération par points. En effet, lorsque $a$ décrit un élément de $\Sigma$, on peut regarder ce point comme se mouvant sur la tangente X en cet élément; pendant ce temps la conique $C_a$ pivote autour du foyer $x$ de cette tangente, en sorte que ce point $x$ appartient à $\Sigma_1$.

Ainsi :

*La transformée d'une ligne est l'enveloppe des coniques conjuguées*

*des points de cette ligne, ou, ce qui revient au même, le lieu géométrique des foyers des tangentes à cette ligne.*

**10.** L'esprit général de cette méthode de transformation est donc de transformer les points en sections coniques circonscrites au triangle invariable et les droites en points.

Un polygone rectiligne de $n$ côtés donnera naissance à un polygone de même nombre de côtés, dont les côtés seront des arcs de sections coniques circonscrites au triangle invariable; on peut lui donner le nom de *polygone conique*.

**11.** Il est évident que toute droite qui passe par un point double a pour foyer ce point lui-même, et par conséquent se transforme en ce point. Donc autant on pourra mener, par un point double, de tangentes à la courbe $\Sigma$, autant de fois $\Sigma_1$ passera par ce point double.

Ainsi, lorsque $\Sigma$ est du degré $m$, $\Sigma_1$ passe $m(m-1)$ fois par chacun des points doubles, en sorte que les points doubles sont généralement des points multiples des transformées.

Désignons par $m$ le degré de la transformée. Par un point quelconque $a$ du plan, on pourra mener à $\Sigma$, $m(m-1)$ tangentes à chacune desquelles correspondra son foyer, point de la transformée $\Sigma_1$ situé sur $C_a$. Donc une conique circonscrite au triangle invariable rencontre $\Sigma_1$ en $m(m-1)$ points, indépendamment des points doubles; et le nombre total des points de rencontre de cette conique avec $\Sigma_1$ est égal à $4m(m-1)$. D'ailleurs ce nombre de points est représenté par $2m_1$, on a donc

$$2m_1 = 4m(m-1),$$

d'où

$$m_1 = 2m(m-1).$$

Telle est la relation qui existe entre le degré d'une courbe et celui de sa transformée.

**12.** Le foyer d'une droite double étant indéterminé et situé en un point quelconque de cette droite, il est clair que lorsque $\Sigma$ touchera une droite double, cette droite appartiendra tout entière à la transformée $\Sigma_1$.

Ainsi un contact de $\Sigma$ avec une droite double introduit cette droite dans la transformée, qui se compose alors de cette droite double et d'une courbe compagne du degré $2m(m-1)-1$ lorsque $\Sigma$ est du degré $m$. Cette courbe compagne passe $m(m-1)$ fois par le point double opposé à la droite double que l'on considère et $m(m-1)-1$ fois par chacun des deux autres sommets du triangle invariable.

Abstraction faite des droites doubles introduites dans la transformée, le degré de cette courbe est réduit d'une unité par chaque contact de $\Sigma$ avec un côté du triangle invariable, en sorte qu'une conique inscrite dans le triangle invariable se transforme en une droite.

## § IV. — *Application de cette méthode à la transformation des sections coniques.*

**13.** Lorsque le degré de $\Sigma$ est égal à 2, celui de $\Sigma_1$ est en général égal à 4. Les coniques se transforment ainsi en lignes du quatrième degré, passant deux fois par chacun des sommets du triangle invariable, en sorte que ces lignes ont nécessairement trois points multiples dont deux peuvent être imaginaires.

Supposons qu'il s'agisse d'un point double réel, et voyons de quelle nature sera le point multiple correspondant.

Si ce point est extérieur à la conique $\Sigma$, on pourra mener par ce point deux tangentes à cette ligne ; ces deux lignes ont le même foyer, le point double lui-même, et c'est ainsi que ce point se trouve appartenir à la fois à deux branches distinctes de la transformée ; on aura un *point multiple ordinaire.*

Si le point double est sur la conique, les deux tangentes sont réelles, mais non plus distinctes : aussi les deux branches de courbe qui viennent concourir au point double se raccordent, et l'on obtient un *point de rebroussement.*

Enfin, lorsque le point double est intérieur à la conique, les deux tangentes sont imaginaires, les deux branches de courbe le sont aussi, et l'on obtient un *point isolé.*

**14.** Il y aurait plusieurs observations à faire sur les constructions géométriques au moyen desquelles on pourrait passer de $\Sigma$ à $\Sigma_1$ ; mais

le but des méthodes de transformation du genre de celle qui nous occupe étant surtout de découvrir des extensions de théorèmes et non des procédés de tracés graphiques, nous n'insisterons pas sur ce point. Nous allons examiner quelles conséquences on peut tirer des théorèmes de Brianchon et de Pascal.

Pour donner à nos phrases plus de clarté et de concision, nous adopterons la dénomination de *conique génératrice*, pour désigner une conique circonscrite au triangle invariable, et nous ferons usage de l'expression *polygone conique*, dans le sens que nous lui avons attribué précédemment (n° **10**).

**15.** Cela posé, considérons une conique $\Sigma$ et un hexagone inscrit quelconque H; les points de concours des côtés opposés de cet hexagone, au nombre de trois, sont sur une ligne droite $X$.

Par la transformation, $\Sigma$ devient une courbe du quatrième ordre $\Sigma_1$ dont chacun des points doubles est un point singulier; l'hexagone inscrit H devient un hexagone conique $H_1$ circonscrit à $\Sigma_1$, les points de concours des côtés opposés de H deviennent les diagonales coniques de $H_1$, et la droite $X$, sur laquelle sont les trois points de concours, devient un point $x$ par lequel passent les trois diagonales coniques.

Ainsi la courbe $\Sigma_1$ et un hexagone circonscrit conique $H_1$ forment une figure telle, que les trois diagonales coniques de l'hexagone passent par un même point $x$.

**16.** Si nous prenons maintenant une conique $\Sigma$ et un hexagone circonscrit quelconque K, les diagonales de cet hexagone, au nombre de trois, concourront en un point $y$.

Par une transformation analogue à la précédente, on trouve que la courbe $\Sigma_1$ et un hexagone inscrit conique $K_1$ forment une figure telle, que les trois points de concours des côtés coniques opposés de cet hexagone sont sur une même conique génératrice $C_y$.

**17.** Les deux propriétés hexagonales de la courbe $\Sigma_1$, qui viennent d'être ainsi établies, peuvent servir à la construction de cette courbe, de la même façon que les propriétés hexagonales des coniques, établies

par les théoremes de Brianchon et de Pascal servent à la construction de ces lignes.

Mais pour que ces propriétés offrent un intérêt réel, il faut faire voir que la transformée $\Sigma_1$ d'une conique $\Sigma$ est une courbe que l'on peut définir indépendamment de toute considération transformatrice. C'est ce qu'on peut aisément établir comme il suit.

Une courbe du quatrième degré est déterminée par quatorze points, et un point multiple à deux branches doit être regardé comme équivalent à trois points. Si donc on veut déterminer une courbe du quatrieme ordre ayant trois points multiples donnés, il faut prendre arbitrairement cinq points $a$, $b$, $c$, $d$, $e$ de cette ligne.

Cela posé, établissons un système de transformation homographique assujetti seulement à la condition que les trois points multiples forment les sommets de son triangle invariable. (Ce système peut être choisi d'une infinité de manières.)

Prenons au moyen de ce système, d'après ce qui a été dit au § I[er], les directrices A, B, C, D, E des cinq points donnés, et construisons la conique $\Sigma$ tangente à ces cinq droites.

Il est facile de voir que la transformée $\Sigma_1$ de cette conique sera précisément la courbe du quatrième degré cherchée.

Par conséquent :

*Toute courbe du quatrième degré à trois points singuliers peut être regardée comme une transformée de conique.*

Une pareille courbe jouit donc des propriétés hexagonales ci-dessus énoncées.

## § V. — *Propriétés de certaines courbes des degrés* 1, 2, 3 *ou* 4.

**18.** Il résulte du paragraphe précédent que lorsqu'une courbe du quatrieme degré possède trois points singuliers, le triangle formé par ces trois points (dont un couple peut être imaginaire), peut être employé très-élégamment pour la construction de cette courbe ; nous donnerons à ce triangle le nom de *triangle générateur*.

Une conique circonscrite à ce triangle portera le nom de *conique génératrice*.

L'expression *polygone conique* désignera un polygone dont les côtés et les diagonales seront formés par des arcs de coniques génératrices.

**19.** D'après cela les théorèmes de Brianchon et de Pascal, étendus aux courbes du quatrième degré, par la méthode de transformation précédente, s'exprimeront très-simplement comme il suit.

Extension du théorème de Pascal :

*Un hexagone conique étant inscrit dans une courbe du quatrième degré à triangle générateur, les trois points de rencontre des couples des côtés opposés sont sur une conique génératrice.*

Extension du théorème de Brianchon :

*Un hexagone conique étant circonscrit à une courbe du quatrième degré à triangle générateur, les trois diagonales coniques passent par un même point.*

**20.** Une courbe du troisième degré peut être déterminée par un point singulier et six points ordinaires.

Formons un triangle avec le point singulier et deux autres points quelconques d'une pareille courbe. La droite qui joindra ces deux derniers points étant associée à la courbe du troisième degré, on aura une courbe du quatrième degré dans laquelle le triangle dont il s'agit sera évidemment *générateur*.

On voit ainsi comment les théorèmes précédents s'appliquent aux lignes du troisième degré, formant une famille caractérisée par l'existence d'un point singulier.

**21.** Prenons maintenant une conique et formons un triangle ayant deux de ses sommets sur cette ligne, le troisième étant quelconque.

La conique et les deux côtés du triangle distincts de sa corde forment une ligne du quatrième degré dont le triangle est *générateur*.

Cette observation applique aux sections coniques les deux théorèmes précédents.

Si l'on suppose que le sommet arbitraire du triangle soit pris sur la corde de la conique, on retombe sur les théorèmes proprement dits de Brianchon et de Pascal.

**22**. Enfin les côtés d'un triangle quelconque et une droite quelconque du plan forment encore une ligne du quatrième degré, dont ce triangle est générateur.

Par cette observation on est conduit à énoncer deux propriétés de la droite.

**23**. Il peut arriver qu'un triangle générateur ait pour sommets un point quelconque et les deux points imaginaires d'intersection de la droite à l'infini avec tous les cercles du plan; les coniques génératrices se réduisent alors à des cercles passant par le premier point.

**24**. En résumé les théorèmes énoncés au numéro **19** s'appliquent aux courbes du quatrième degré à trois points singuliers, aux courbes du troisième degré qui présentent un point singulier, à toutes les coniques et à toutes les droites, à la condition qu'on choisisse convenablement le triangle générateur.

Ce triangle, entièrement déterminé dans le premier cas, prend une indétermination de plus en plus grande lorsqu'on passe aux cas suivants et devient tout à fait arbitraire quand on arrive au dernier cas.

# THÉORÈMES

CONCERNANT

## LE QUINTUPLE D'UN NOMBRE PREMIER DE LA FORME $24k+17$;

**Par M. J. LIOUVILLE.**

Nous considérons ici le quintuple d'un nombre premier $m$ de la forme $24k+17$. Le nombre N de manières dont on peut poser, pour chaque entier $m$ de l'espèce indiquée, l'équation

$$5m = 2x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs et $p$ un nombre premier non diviseur de $y$, est essentiellement pair, mais au moins égal à 2. Cela résultera des deux théorèmes qui font l'objet de cet article. On va le voir en effet, N est la somme de deux nombres impairs $N_1$, $N_2$ qui répondent respectivement aux deux hypothèses distinctes de $x$ divisible par 3 et de $x$ premier à 3. Quant à $y$, on s'assurera sans peine qu'il n'est jamais divisible par 3.

*Théorème I.* — « Pour tout nombre premier donné $m$, de la forme » $24k+17$, on peut poser au moins une fois (et toujours un nombre » impair de fois) l'équation

$$5m = 18x^2 + p^{4l+1}y^2,$$

» $x$ et $y$ étant des entiers impairs et $p$ un nombre premier non diviseur de $y$. »

Le nombre premier $p$, qui figure au second membre de l'équation

$$5m = 18x^2 + p^{4l+1}y^2,$$

doit, dans les conditions où nous nous sommes placés, vérifier les

deux congruences

$$p \equiv 3 \pmod{8}, \qquad p \equiv 1 \pmod{3};$$

il ne peut donc être que de la forme $24g + 19$.

Les exemples les plus simples sont ceux de

$$m = 17, \quad m = 41, \quad m = 89.$$

Pour chacun des nombres que je viens d'écrire, on trouve une équation canonique, savoir

$$5.17 = 18.1^2 + 67.1^2,$$

puis

$$5.41 = 18.3^2 + 43.1^2,$$

enfin

$$5.89 = 18.3^2 + 283.1^2.$$

Même vérification pour

$$m = 113, \quad m = 137:$$

car on a

$$5.113 = 18.1^2 + 547.1^2,$$

et

$$5.137 = 18.3^2 + 523.1^2.$$

Nous ne pousserons pas plus loin les exemples.

*Théorème II.* — « Pour tout nombre premier donné $m$, de la » forme $24k + 17$, on peut poser au moins une fois (et toujours un » nombre impair de fois) l'équation

$$5m = 2x^2 + p^{4l+1}y^2,$$

» $x$ et $y$ étant des entiers impairs, non divisibles par 3, et $p$ un » nombre premier qui ne divise pas $y$. »

Dans les conditions spéciales de cet énoncé, le nombre premier $p$

doit vérifier les deux congruences

$$p \equiv 3 \pmod{8}, \qquad p \equiv 2 \pmod{3};$$

il ne peut donc être que de la forme $24g + 11$.

Vérifions à son tour le théorème II, en prenant d'abord

$$m = 17,$$

puis

$$m = 41.$$

Pour chacun de ces deux nombres, on trouve une équation canonique :

$$5.17 = 2.1^2 + 83.1^2,$$

puis

$$5.41 = 2.7^2 + 107.1^2.$$

On a trois équations canoniques pour

$$m = 89,$$

savoir

$$5.89 = 2.1^2 + 443.1^2,$$
$$5.89 = 2.7^2 + 347.1^2,$$
$$5.89 = 2.13^2 + 107.1^2;$$

trois aussi pour

$$m = 113,$$

car

$$5.113 = 2.1^2 + 563.1^2,$$
$$5.113 = 2.7^2 + 467.1^2,$$
$$5.113 = 2.13^2 + 227.1^2.$$

Ces exemples suffiront

# THÉORÈME

CONCERNANT

LES NOMBRES PREMIERS DE L'UNE OU DE L'AUTRE DES DEUX FORMES $120k+61$, $120k+109$;

PAR M. J. LIOUVILLE.

Soit $m$ un nombre premier donné, de l'une ou de l'autre des deux formes

$$120k+61, \qquad 120k+109.$$

Nous aurons pour le nombre $m$ dont il s'agit ce théorème, que l'on peut poser au moins une fois (et toujours un nombre impair de fois) l'équation

$$m = 30x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs et $p$ un nombre premier ($120g+31$ ou $120g+79$) non diviseur de $y$ : on admet pour $l$ la valeur zéro.

En d'autres termes, si d'un nombre premier $m$, de l'une ou de l'autre des deux formes $120k+61$, $120k+109$, on retranche, tant que faire se peut, les entiers compris dans la suite

$$30.1^2,\ 30.3^2,\ 30.5^2,\ldots,$$

il y aura un nombre impair de restes susceptibles d'être mis sous la forme

$$p^{4l+1}y^2,$$

$p$ étant un nombre premier non diviseur de $y$. Quant à la forme linéaire ($120g+31$ ou $120g+79$) que nous attribuons à $p$, c'est une

conséquence immédiate de notre équation

$$m = 30x^2 + p^{4l+1}y^2,$$

qui, dans les conditions où nous nous sommes placés, entraine ces trois congruences :

$$p \equiv 7 \pmod{8}, \qquad p \equiv 1 \pmod{3}, \qquad p \equiv \pm 1 \pmod{5}.$$

Donnons quelques exemples numériques, en considérant successivement les nombres premiers $m$ de la forme $120k + 61$, puis les nombres premiers $m$ de la forme $120k + 109$.

Les nombres premiers les plus petits de la forme

$$120k + 61,$$

sont 61, 181, 421, 541, 661; et pour chacun d'eux on peut écrire une seule équation canonique, savoir

$$61 = 30.1^2 + 31.1^2,$$
$$181 = 30.1^2 + 151.1^2,$$
$$421 = 30.3^2 + 151.1^2,$$
$$541 = 30.3^2 + 271.1^2,$$
$$661 = 30.1^2 + 631.1^2.$$

On n'a pas d'équation canonique en retranchant 30 de 421 et de 541, ni en retranchant $30.3^2$, ou 270, de 661. En effet, des trois restes qu'on obtient ainsi, le second, 511, est le produit des deux nombres premiers 7 et 73, et les deux autres sont égaux à 391, c'est-à-dire à 17.23.

Même vérification de notre théorème pour les nombres premiers de la forme

$$120k + 109.$$

Les trois plus petits sont 109, 229, 349; et l'on a les équations cano-

niques

$$109 = 30.1^2 + 79.1^2.$$

$$229 = 30.1^2 + 199.1^2.$$

$$349 = 30.3^2 + 79.1^2.$$

On n'en obtient pas en retranchant 30 de 349, attendu que le reste, 319, est le produit des deux nombres premiers 11 et 29.

Soit, pour terminer,

$$m = 709,$$

et nous verrons que là encore notre théorème est vérifié, à cause de l'équation canonique

$$709 = 30.3^2 + 439.1^2.$$

# NOUVELLE THÉORIE

DES

# FONCTIONS DE VARIABLES IMAGINAIRES;

PAR M. MAXIMILIEN MARIE,
Ancien élève de l'École Polytechnique.

## TROISIÈME PARTIE.

DE LA MARCHE DES VALEURS D'UNE FONCTION IMPLICITE DÉFINIE PAR UNE ÉQUATION ALGÉBRIQUE.

(Suite.)

## CHAPITRE VIII.

*De la marche des valeurs d'une fonction de plusieurs variables et de la convergence du développement de cette fonction suivant la formule de Taylor.*

**118.** La question que nous avons traitée dans le chapitre VI a été posée par M. Cauchy pour servir d'introduction à des recherches ultérieures sur les périodes des intégrales.

Après avoir résolu les questions qui se rapportent aux périodes des intégrales simples, M. Cauchy a tenté d'appliquer ses méthodes à l'étude des intégrales d'ordres supérieurs.

Peut-être l'illustre maître n'a-t-il consacré que trop peu d'efforts à ces nouvelles recherches; peut-être a-t-il pensé que la manière dont il figurait la marche de la variable indépendante, en géométrie plane, ne conviendrait plus au cas où la fonction dépendrait de deux ou d'un plus grand nombre de variables.

Quoi qu'il en soit, on n'avait jusqu'ici rien proposé relativement

aux périodes des intégrales d'ordres supérieurs, et il ne paraît même pas que la question de la marche d'une fonction implicite de plusieurs variables, question qui, conformément au programme de M. Cauchy, eût dû précéder, ait reçu un commencement de solution.

Cette question cependant ne présentera aucune difficulté nouvelle, la méthode que nous avons développée dans le chapitre VI s'y appliquera, sans presque subir de modifications, et le passage même sera assez facile.

La question, restreinte au cas des fonctions de deux variables indépendantes, peut être posée de trois manières différentes : nous commencerons par les distinguer.

Soit

$$f(x, y, z) = 0$$

l'équation qui définit $z$ implicitement. On pourra d'abord supposer que $x$ et $y$ partant des valeurs initiales $x_0$, $y_0$, $z$ parte en même temps d'une de ses valeurs correspondantes, $z_0$, et demander ce que deviendra $z$, assujetti à la loi de continuité, lorsque $x$ et $y$ passeront d'une manière continue, de leurs valeurs initiales $x_0$, $y_0$, à des valeurs quelconques $x_1$, $y_1$, en suivant un chemin défini par *trois* équations entre leurs parties réelles et imaginaires.

Le second cas dont aurons à nous occuper sera celui où l'on ne donnerait plus que *deux* équations entre les quatre parties qui composent $x$ et $y$.

Dans le cas précédent, lorsqu'on se serait donné l'une des variables indépendantes, toutes les autres eussent été, par là même, déterminées, tandis que, dans le cas actuel, si l'on attribue une valeur arbitraire à l'une des variables indépendantes, ou, plus généralement, si l'on introduit entre les six variables une relation complémentaire arbitrairement choisie, l'ensemble des solutions communes aux équations formulées représentera une ligne

Or cette ligne devant être en général composée de plusieurs branches, on pourra se proposer, connaissant les deux formes initiale et finale de la relation complémentaire et la loi suivant laquelle elle a passé de l'une à l'autre, de déterminer, sur le lieu final, la branche qui serait provenue d'une branche désignée du lieu initial, cette

branche n'ayant pu se déplacer et se déformer que d'une manière continue.

Enfin nous supposerons que les parties réelles et imaginaires de $x$ et de $y$ ne soient plus liées entre elles que par une seule équation permanente : si alors on introduit entre les six variables une relation complémentaire arbitraire et variable de forme, les solutions communes aux équations considérées représenteront une surface, composée en général de plusieurs nappes, et l'on pourra se proposer de déterminer, dans le lieu défini par l'équation complémentaire, arrivée à sa forme finale, la nappe qui serait provenue d'une nappe définie du lieu initial, par déplacement et déformation continus.

La question se décompose donc en trois autres bien distinctes.

Dans la première, le cas pratique sera celui où des trois relations qu'on doit fournir entre les parties réelles et imaginaires de $x$ et de $y$ deux seraient données par une équation entre $x$ et $y$, la troisième $\varphi(\alpha, \beta) = 0$ définissant le chemin que devra suivre $x$.

Dans la seconde, pour s'écarter le moins possible de la réalité, il faudra de même donner par une équation entre $x$ et $y$ les deux conditions que devront remplir les parties réelles et imaginaires de ces deux variables.

Enfin dans la troisième, pour les mêmes motifs, nous examinerons principalement le cas où la relation qu'on devrait donner serait définie par une équation entre $x$ et $y$, mais contenant une constante arbitraire réelle.

On eût pu chercher à ramener les trois questions à la dernière, qui comprend en effet les deux autres par sa plus grande généralité ; mais ce seront au contraire les deux dernières que nous ramènerons à la première, parce qu'en effet, pour que la nappe considérée du lieu initial soit venue se confondre avec une nappe désignée du lieu final, dans la dernière question, il faudra que la branche, contenue sur la nappe initiale, d'un lieu curviligne défini par l'introduction d'une nouvelle équation, soit venue se superposer à la branche, contenue sur la nappe finale, du même lieu curviligne mobile ; de même que la première branche ne sera venue se placer sur la seconde, qu'autant que les points de l'une seront venus occuper la place des points de l'autre.

En sorte qu'en général les deux dernières questions pourront être

considérées comme résolues lorsque la première le sera ; avec cette restriction toutefois que, comme la nappe considérée du lieu initial, dans le dernier cas, ou la branche considérée, dans le second, pourraient se scinder à un certain moment et fournir dans le lieu final des nappes ou branches séparées, ou qu'il convint de distinguer, il ne suffira pas, en général, d'avoir étudié le mouvement d'un seul point $[x, y, z]$ du lieu mobile, pour pouvoir conclure d'une manière certaine à l'égard des deux dernières questions.

**119.** *De la marche des valeurs d'une fonction de deux variables imaginaires assujetties à trois conditions.* — La question qui va nous occuper n'est pas seulement de l'ordre de celles que nous avons traitées dans le chapitre VI; car si deux des trois équations qui doivent regler la marche des variables indépendantes $x$ et $y$, dont dépend la fonction $z$, étaient renfermées dans une équation entre $x$ et $y$, l'autre ne contenant d'ailleurs que les parties réelle et imaginaire de $x$, par exemple, l'élimination préalable de $y$ ferait même disparaître toute espèce de différence.

Cette élimination sera toujours permise et devra même être pratiquée dans tous les cas où elle sera possible ; mais nous n'y recourrons pas dans nos explications générales.

**120.** Si la fonction $z$ n'entrait qu'au second degré dans l'équation

$$f(x, y, z) = 0,$$

qui la définit, elle s'exprimerait par

$$z = P \pm \sqrt{Q},$$

P et Q étant deux fonctions rationnelles de $x$ et de $y$ : l'évaluation de P ne pouvant donner lieu à aucune ambiguïté, ce serait, en conséquence, sur $z - P$ que devrait porter la discussion.

Or les parties réelle et imaginaire de $z - P$ ne pouvant changer de signe qu'en passant par zéro, ou par l'infini (on pourrait toujours, par une transformation de variables, écarter à l'avance, si on le voulait, le cas où $z$ aurait à passer par des valeurs infinies), la valeur qu'aura dû

prendre la fonction $z - P$, assujettie à la loi de continuité, lorsque $x$ et $y$ auront passé d'une manière continue, par le chemin convenu, de leur état initial à leur état final, cette valeur sera toujours facile à assigner, lorsqu'on aura suivi les variations de signe d'une des parties de la fonction.

Si le chemin parcouru par le système des variables $x$ et $y$ est fermé, les deux valeurs de $z$ s'échangeront entre elles, lorsque la partie qu'on aura étudiée de $z - P$ aura changé de signe un nombre impair de fois, tandis que, dans le cas contraire, chacune des fonctions reprendra sa valeur initiale.

**121**. Supposons, par exemple, qu'il s'agisse de la fonction $z$ définie par l'équation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1$$

qui donne

$$\frac{z}{c} = \pm \sqrt{1 - \frac{x^2}{a^2} - \frac{y^2}{b^2}};$$

nous poserons comme toujours

$$x = \alpha + \beta\sqrt{-1},$$

$$y = \alpha' + \beta'\sqrt{-1},$$

$$z = \alpha'' + \beta''\sqrt{-1},$$

la condition de réalité de $z$ étant

$$\frac{\alpha\beta}{a^2} + \frac{\alpha'\beta'}{b^2} = 0 \quad \text{avec} \quad 1 - \frac{\alpha^2 - \beta^2}{a^2} - \frac{\alpha'^2 - \beta'^2}{b^2} > 0,$$

et celle qui en ferait disparaître la partie réelle étant

$$\frac{\alpha\beta}{a^2} + \frac{\alpha'\beta'}{b^2} = 0 \quad \text{avec} \quad 1 - \frac{\alpha^2 - \beta^2}{a^2} - \frac{\alpha'^2 - \beta'^2}{b^2} < 0,$$

les points importants de la discussion porteront sur les passages de

$\alpha$, $\beta$, $\alpha'$, $\beta'$ par des valeurs dont le système satisfît à la condition

$$\frac{\alpha\beta}{a^2}+\frac{\alpha'\beta'}{b^2}=0.$$

Or celle des parties de $z$ qui s'annulera en même temps que

$$\frac{\alpha\beta}{a^2}+\frac{\alpha'\beta'}{b^2}$$

changera de signe avec cette quantité; en sorte que tout se réduira, à chaque passage, à savoir si

$$\frac{\alpha\beta}{a^2}+\frac{\alpha'\beta'}{b^2}$$

aura ou non changé de signe en passant par zéro, ce qui sera toujours aisé puisque ayant entre $\alpha$, $\beta$, $\alpha'$ et $\beta'$ trois relations connues, qui pourront fournir $\frac{d\beta}{d\alpha}$, $\frac{d\alpha'}{d\alpha}$ et $\frac{d\beta'}{d\alpha}$ en fonction de $\alpha$, $\beta$, $\alpha'$, $\beta'$, on pourra connaître le sens dans lequel aura varié

$$\frac{\alpha\beta}{a^2}+\frac{\alpha'\beta'}{b^2}.$$

**122** La question analytique étant ainsi traitée, il nous reste à étudier le caractère concret de la condition

$$\frac{\alpha\beta}{a^2}+\frac{\alpha'\beta'}{b^2}=0:$$

elle exprime que le point $[x, y, z]$ passe sur une conjuguée dont les $z$ sont réels, ou imaginaires sans parties réelles; mais ce point demande quelques éclaircissements.

Concevons par l'axe des $z$ un plan mobile

$$y = mx,$$

ayant pour coefficient angulaire le rapport variable $\frac{\beta}{\beta'}$, prenons à chaque instant sa trace pour axe des $x$ et, pour axe des $y$, le diamètre

conjugué

$$y = -\frac{b^2}{a^2 m} x$$

de la section horizontale.

$z$, dans cette transformation, ne changera pas; pour ne pas multiplier inutilement les notations, continuons de représenter par $x$ et $y$ les coordonnées horizontales de la surface : $y$ sera maintenant constamment réel et $x$ restera représenté par $\alpha + \beta\sqrt{-1}$; $x$, $y$, $z$ seront d'ailleurs liés entre eux par une nouvelle équation

$$\frac{x^2}{a'^2} + \frac{y^2}{b'^2} + \frac{z^2}{c^2} - 1 = 0,$$

dans laquelle $a'$ et $b'$ dépendront de $m$.

La condition de réalité de $z$ sera maintenant

$$\alpha\beta = 0 \quad \text{avec} \quad 1 - \frac{\alpha^2 - \beta^2}{a'^2} - \frac{y^2}{b'^2} > 0.$$

et la condition pour que $z$ manque de partie réelle

$$\alpha\beta = 0 \quad \text{avec} \quad 1 - \frac{\alpha^2 - \beta^2}{a'^2} - \frac{y^2}{b'^2} < 0.$$

ou, en décomposant : les conditions de réalité de $z$ seront

$$\alpha = 0 \quad \text{avec} \quad 1 + \frac{\beta^2}{a'^2} - \frac{y^2}{b'^2} > 0.$$

ou

$$\beta = 0 \quad \text{avec} \quad 1 - \frac{\alpha^2}{a'^2} - \frac{y^2}{b'^2} > 0;$$

et les conditions pour que $z$ manque de partie réelle,

$$\alpha = 0 \quad \text{avec} \quad 1 + \frac{\beta^2}{a'^2} - \frac{y^2}{b'^2} < 0.$$

ou

$$\beta = 0 \quad \text{avec} \quad 1 - \frac{\alpha^2}{a'^2} - \frac{y^2}{b'^2} < 0.$$

Cela posé, le plan parallèle aux $xz$, mené à la distance $y$, coupera la surface suivant une ellipse réelle et toutes ses conjuguées hyperboliques, si $y^2$ est moindre que $b'^2$, et, dans le cas contraire, suivant des hyperboles ayant pour enveloppe une ellipse imaginaire.

Or si d'abord nous supposons $y^2$ moindre que $b'^2$, quand $\alpha$ passera par zéro,

$$1+\frac{\beta^2}{a'^2}-\frac{y^2}{b'^2}$$

sera nécessairement positif et le point $[x, z]$ se trouvera, dans le plan que nous supposons, sur l'hyperbole imaginaire dont les $z$ sont réels, dont l'axe transverse, par conséquent, est parallèle aux $z$:

Et quand $\beta$ passera par zéro, le point $[x, z]$ sera sur l'ellipse réelle, si

$$1-\frac{\alpha^2}{a'^2}-\frac{y^2}{b'^2}$$

est positif, ou, dans le cas contraire, sur la conjuguée dont l'axe transverse est parallèle aux $x$.

En second lieu si nous supposons $y^2$ plus grand que $b'^2$, quand $\alpha$ passera par zéro, le point $[x, z]$ se trouvera sur la conjuguée dont l'axe transverse est parallèle aux $z$, si

$$1+\frac{\beta^2}{a'^2}-\frac{y^2}{b'^2}$$

est positif, et sur l'enveloppe imaginaire dans le cas contraire :

Et quand $\beta$ passera par zéro,

$$1-\frac{\alpha^2}{a'^2}-\frac{y^2}{b'^2}$$

étant necessairement négatif, le point $[x, z]$ se trouvera sur la conjuguée dont l'axe transverse est parallèle aux $x$.

Cela posé, nous pouvons répéter ici les mêmes observations que nous avons présentées, dans le cas analogue, en géométrie plane.

Supposons que $x$ et $y$ reviennent à leur état primitif. Si $\alpha$ a passé par zéro, il aura dû changer de signe un nombre pair de fois: à chaque fois la partie réelle aura changé de signe, par conséquent il

n'y aura pas d'effet produit dans la valeur de $z$; mais si $\beta$ a passé par zéro et changé de signe deux fois, l'une avec la circonstance

$$1 - \frac{\alpha^2}{a'^2} - \frac{y^2}{b'^2} > 0,$$

et l'autre avec la circonstance contraire, les parties imaginaire et réelle de $z$ auront successivement changé de signe et les deux valeurs de $z$ se seront permutées.

**123.** Si l'équation proposée contenait la fonction $z$ à un degré supérieur au second, le calcul pourrait présenter des difficultés plus considérables ; mais la méthode serait encore pareille à celle que nous avons appliquée, en géométrie plane, au cas analogue.

On classerait toujours les conjuguées de la surface proposée en deux catégories, suivant que ces conjuguées toucheraient ou non la surface réelle.

Les conjuguées tangentes à la surface réelle se diviseraient en plusieurs classes, selon qu'elles toucheraient cette surface sur telle ou telle nappe.

Chaque conjuguée tangente à la surface réelle serait divisée en parties distinctes par la courbe de contact.

Or le point $[x, y]$ ne pourrait passer d'une catégorie de conjuguées à l'autre, sans prendre son passage sur une conjuguée limite commune des deux catégories; ces passages devraient être relevés avec soin.

Il ne pourrait non plus passer d'une classe de conjuguées d'une même catégorie à une autre classe, sans prendre passage sur une conjuguée limite commune des deux classes.

Enfin il ne pourrait passer d'une partie à une autre d'une conjuguee, sans passer sur la surface réelle.

Quant aux conjuguées non tangentes à la surface réelle, elles donneraient lieu à une discussion plus compliquée; mais on pourra appliquer au cas où le point $[x, y, z]$ aurait passé sur ces conjuguées, une autre méthode d'ailleurs générale.

**124.** On pourra, si on le veut, comme nous l'avons fait pour étu-

dier l'équation

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}=1,$$

faire suivre au plan des $xz$ le mouvement du plan

$$y=\frac{\beta}{\beta'}x,$$

ce qui rendra $y$ perpétuellement réel, et étudier la marche du point $[x, z]$ dans le plan mené parallèlement à celui des $xz$ à une distance égale au nouvel $y$.

La question alors sera ramenée à une question de géométrie plane qui ne différerait de celle que nous avons traitée dans le chapitre VI qu'en ce que les équations données entre $z$ et $x$ contiendraient des variables intermédiaires et seraient, par suite, en plus grand nombre.

**125.** *De la marche des valeurs d'une fonction de deux variables imaginaires assujetties à deux conditions.* — Les solutions communes à l'équation caractéristique

$$f(x, y, z)=0$$

et à deux autres équations permanentes

$$F(\alpha, \beta, \alpha', \beta')=0, \quad F_1(\alpha, \beta, \alpha', \beta')=0,$$

formeraient un système doublement indéterminé, auquel par conséquent correspondrait une surface. Mais si l'on joint à ces équations une condition mouvante

$$\varphi(\alpha, \beta)=0,$$

les solutions communes ne fourniront plus qu'une ligne courbe, pour chaque forme de l'équation $\varphi$. On pourra donc chercher à savoir comment une branche désignée de cette courbe se déplacera et se déformera, lorsque la fonction $\varphi$ se déformera elle-même; on pourra, en particulier, demander ce qu'une branche désignée de la courbe primi-

tive serait devenue en passant de l'équation

$$\varphi_0(\alpha, \beta) = 0$$

à l'équation

$$\varphi_1(\alpha, \beta) = 0.$$

Telle serait dans toute sa généralité la question que nous aurions à étudier dans ce paragraphe.

Comme nous la ramenons à savoir ce que sont devenus les points de la branche assignée de la courbe définie par les équations

$$f(x, y, z) = 0,$$
$$F(\alpha, \beta, \alpha', \beta') = 0, \quad F_1(\alpha, \beta, \alpha', \beta') = 0,$$
$$\varphi_0(\alpha, \beta) = 0,$$

il nous suffira de montrer par un exemple comment cette réduction peut s'effectuer.

Soit

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} - 1 = 0$$

l'équation qui lie la fonction $z$ aux deux variables $x$ et $y$;

$$\beta' = 0, \quad \text{c'est-à-dire} \quad y = \text{réel},$$

l'une des deux conditions que l'on devait fournir entre $x$ et $y$; enfin supposons que la seconde condition soit donnée par le système

$$\left\{\begin{aligned} x^2 + y^2 &= r^2, \\ r &= \rho + \rho'\sqrt{-1}, \\ \rho^2 + \rho'^2 &= ab; \end{aligned}\right.$$

et faisons passer $\rho'$ et $\rho$ par toutes les valeurs que prendraient successivement les coordonnées d'un mobile assujetti à décrire de droite à gauche la circonférence du cercle

$$y^2 + x^2 = ab,$$

et qui, partant du point situé sur la partie positive de l'axe des $x$, y reviendrait après un tour complet.

A chaque valeur de $\rho'$, il correspondra une valeur de $\rho$, par suite une valeur de $r$; les solutions communes aux deux équations

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} - 1 = 0,$$

$$x^2 + y^2 = r^2$$

fourniraient une surface, mais la condition $y =$ réel réduira ce lieu à une ligne.

A l'origine du mouvement, c'est-à-dire lorsque $\rho'$ était nul et $\rho$ egal a $+\sqrt{ab}$, la ligne mobile sera composée d'une courbe d'entrée et d'une courbe de sortie; à la fin du mouvement, la ligne mobile sera revenue occuper sa position initiale : la question serait donc de savoir quelles permutations auront pu se produire entre les branches de cette courbe, du commencement à la fin du mouvement.

Pour traiter cette question conformément au plan tracé dans les applications qui précèdent, il nous suffira, puisque $y$ doit rester constamment réel, d'étudier le mouvement du point de rencontre de la ligne mobile avec un plan réel parallèle aux $xz$,

$$y = h,$$

car en faisant varier $h$, nous pourrons ensuite assigner la position finale d'un point quelconque de la ligne mobile.

L'équation

$$y^2 + x^2 = (\rho + \rho'\sqrt{-1})^2$$

représente les cylindres parallèles aux $z$ qui auraient pour traces sur le plan des $xy$ les conjuguées du lieu

$$y^2 + x^2 = (\rho + \rho'\sqrt{-1})^2.$$

Ces conjuguées sont toutes égales entre elles; elles ont pour enveloppe imaginaire la circonférence du cercle

$$y^2 + x^2 = (\rho + \rho')^2,$$

mais celle dont les ordonnées sont réelles nous occupera seule.

Cette conjuguée touche l'enveloppe imaginaire aux extrémités du diamètre dirigé suivant l'axe des $x$ et a pour asymptotes les bissectrices des angles des axes; elle se réduit soit à l'hyperbole équilatère, qui a pour axe transverse l'axe des $x$, lorsque $\rho$ s'annule, soit au cercle et à l'hyperbole équilatère, qui a pour axe transverse l'axe des $y$, lorsque c'est au contraire $\rho'$ qui passe par zéro.

Le plan

$$y = h$$

coupe le cylindre

$$y^2 + x^2 = (\rho + \rho' \sqrt{-1})^2$$

suivant les génératrices partant des points d'intersection de la droite $y = h$ avec la conjuguée dont il vient d'être question.

Lorsque $h$ est moindre que $b$, le plan

$$y = h$$

coupe l'ellipsoïde suivant une ellipse réelle dont la projection, en vraie grandeur, sur le plan des $xz$ a pour équation

$$\frac{x^2}{a^2} + \frac{z^2}{c^2} = 1 - \frac{h^2}{b^2},$$

et toutes ses conjuguées.

Tandis que lorsque $h$ est plus grand que $b$, l'intersection se compose des conjuguées de l'enveloppe imaginaire elliptique

$$\frac{x^2}{a^2} + \frac{z^2}{c^2} = -\left(\frac{h^2}{b^2} - 1\right).$$

Cela posé, déterminons d'abord la courbe fournie par le système des équations

$$\begin{cases} \dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} + \dfrac{z^2}{c^2} - 1 = 0, \\ x^2 + y^2 = ab, \\ y = h, \end{cases}$$

dans lequel on ferait passer $h$ par toutes les valeurs réelles de $-\infty$ à $+\infty$.

Lorsque $h$ varie entre $-\sqrt{ab}$ et $+\sqrt{ab}$, $x$ reste réel; quant à $z$, il prend la valeur déterminée par l'équation

$$\frac{z^2}{c^2} = 1 - \frac{ab - y^2}{a^2} - \frac{y^2}{b^2}$$

ou

$$\frac{z^2}{c^2} = (a - b)\frac{ab^2 - (a+b)y^2}{a^2 b^2},$$

il est donc réel ou imaginaire, suivant que $y^2$ est moindre ou plus grand que

$$\frac{ab^2}{a+b},$$

de sorte qu'entre les limites

$$-b\sqrt{\frac{a}{a+b}} < y < +b\sqrt{\frac{a}{a+b}},$$

le lieu est réel et appartient par conséquent à l'ellipsoïde.

Tandis qu'entre les limites

$$-b\sqrt{\frac{a}{a+b}} > y > -\sqrt{ab},$$

ou

$$+b\sqrt{\frac{a}{a+b}} < y < +\sqrt{ab},$$

le lieu est imaginaire; mais ses $x$ et $y$ étant réels, il appartient à l'hyperboloïde à une nappe circonscrit à l'ellipsoïde le long de son contour apparent par rapport au plan des $xy$,

$$\begin{cases} z = 0, \\ \dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} - 1 = 0. \end{cases}$$

Enfin en dehors des limites

$$-\sqrt{ab} \quad \text{et} \quad +\sqrt{ab},$$

les $y$ de la courbe sont réels, ses $x$ sont imaginaires sans parties réelles, et quant à ses $z$, déterminés par l'équation

$$\frac{z^2}{c^2} = (a - b)\frac{ab^2 - (a + b)y^2}{a^2 b^2},$$

ils sont aussi imaginaires, sans parties réelles, puisque $y^2$ surpassant $ab$, à plus forte raison

$$ab^2 - (a + b)y^2$$

est négatif; la courbe appartient donc à l'hyperboloïde à deux nappes

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} + \frac{z^2}{c^2} = -1,$$

qui du reste n'est pas une conjuguée de l'ellipsoïde.

Lorsque

$$y = \pm\sqrt{ab}, \quad x = 0 \quad \text{et} \quad \frac{z^2}{c^2} = 1 - \frac{a}{b},$$

le point

$$x = 0, \quad y = \sqrt{ab}, \quad z = c\sqrt{\frac{a}{b} - 1}$$

appartient donc à la fois, comme cela devait être, aux deux hyperboloïdes

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1$$

et

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1.$$

Cela posé, il ne nous reste qu'à donner successivement à $h$ des valeurs comprises entre o et $+ b\sqrt{\frac{a}{a+b}}$, entre $+ b\sqrt{\frac{a}{a+b}}$ et $+\sqrt{ab}$, enfin entre $+\sqrt{ab}$ et $+\infty$, et à examiner ce qui, dans chaque cas, aura dû se passer lorsque $\rho$ et $\rho'$ seront revenus à leurs valeurs initiales $+\sqrt{ab}$ et o.

Supposons d'abord $h$ compris entre o et $+ b\sqrt{\frac{a}{a+b}}$, le point

$[x, z]$ alors se déplacera sur les conjuguées de l'ellipse

$$\frac{x^2}{a^2} + \frac{z^2}{c^2} = 1 - \frac{h^2}{b^2};$$

s'il était d'abord (c'est-à-dire lorsque $\rho'$ était nul et $\rho$ égal à $+\sqrt{ab}$) sur la nappe supérieure de l'ellipsoïde, $\rho'$ devenant positif, l'équation

$$x dx = r dr,$$

où il faudrait faire $x$ réel et positif, $r$ égal à $+\sqrt{ab}$ et $dr$ égal à $d\rho + d\rho'\sqrt{-1}$, $d\rho'$ étant positif, montre que la partie imaginaire de $dx$ sera positive.

D'un autre côté, l'équation

$$\frac{x\,dx}{a^2} + \frac{z\,dz}{c^2} = 0,$$

où il faudrait faire $z$ réel et positif, montre à son tour que la partie imaginaire de $dz$ sera négative.

Le point $[x, z]$ se placera donc d'abord sur une branche inférieure de conjuguée de l'ellipse

$$\frac{x^2}{a^2} + \frac{z^2}{c^2} = 1 - \frac{b^2}{a^2},$$

il restera d'ailleurs du même côté du point de contact de l'ellipse avec la conjuguée où il pourra se transporter, jusqu'au moment où $\rho'$ repassera par zéro, $\rho$ ayant alors la valeur $-\sqrt{ab}$ : car en vertu de l'équation

$$x^2 = (\rho + \rho'\sqrt{-1})^2 - h^2,$$

$x$ ne peut être réel qu'autant que $\rho'$ est nul.

Mais avant que $\rho'$ ne redevînt nul, $\rho$ lui-même aura passé par zéro, et ce passage doit attirer notre attention.

Au moment où $\rho$ sera devenu nul, $\rho'$ aura pris la valeur $+\sqrt{ab}$, $x$ aura l'une de celles que comprend la formule

$$\pm\sqrt{-1}\sqrt{h^2 + ab}.$$

Mais comme la partie imaginaire de cette variable avait commencé par être positive et qu'elle n'a pas repassé par zéro, la seule valeur admissible sera

$$x = +\sqrt{-1}\sqrt{h^2 + ab}.$$

Quant à $z$, il aura pris l'une des valeurs

$$\pm c\sqrt{1 + \frac{h^2 + ab}{a^2} - \frac{h^2}{b^2}},$$

qui sont réelles, car la condition

$$1 + \frac{h^2 + ab}{a^2} > \frac{h^2}{b^2}$$

revient à

$$ab^2 > h^2(a - b),$$

et $h^2$ étant moindre que $\frac{ab^2}{a+b}$ est, à plus forte raison, inférieur à $\frac{ab^2}{a-b}$.

D'ailleurs la partie réelle de $z$ étant d'abord positive et n'ayant pas encore passé par zéro, sera restee positive, de sorte que la valeur finale de $z$ sera

$$z = +c\sqrt{1 + \frac{h^2 + ab}{a^2} - \frac{h^2}{b^2}};$$

le point $[x, z]$ se trouvera donc alors sur la partie de droite de la branche supérieure de la conjuguée $\frac{\beta''}{\beta} = 0$.

La caractéristique changera de signe aussitôt apres, car, en vertu de l'équation

$$xdx = rdr$$

où il faudrait faire

$$x = +\sqrt{-1}\sqrt{h^2 + ab}, \quad r = +\sqrt{-1}\sqrt{ab},$$

et $d\rho'$ négatif, la partie imaginaire de $dx$ sera négative.

Au moment donc où $\rho'$ sera nul et où $\rho$ prendra la valeur $-\sqrt{ab}$, le point $[x, z]$ devra se trouver sur le second quadrant de l'ellipse

$$\frac{x^2}{a^2}+\frac{z^2}{c^2}=1-\frac{h^2}{b^2}.$$

A partir de là il changera de branche sur la conjuguée où il se transportera, car en vertu de l'équation

$$xdx=rdr$$

où $x$ serait réel et négatif, $r$ égal à $-\sqrt{ab}$, et où $dr$ aurait sa partie imaginaire négative, la partie imaginaire de $dx$ redeviendra négative tandis que, par suite, celle de $dz$ deviendra positive, pour que $\frac{\beta''}{\beta}$ reste négatif, comme cela doit être.

Le point $[x, z]$ restera maintenant sur une branche inférieure de la conjuguée tant que $\rho'$ ne repassera pas par zéro.

Il repassera sur la conjuguée $\frac{\beta''}{\beta}=0$ au moment où $\rho$ redeviendra nul et $\rho'$ égal à $-\sqrt{ab}$; mais comme il n'aura pas pu passer sur la conjuguée $\frac{\beta''}{\beta}=\infty$, puisque $x$ n'aura jamais pu prendre de valeurs réelles supérieures à $a$, les mêmes faits se reproduiront ensuite en sens inverse, de sorte que quand $\rho$ et $\rho'$ auront achevé leur évolution, le point $[x, y]$ reviendra à sa place primitive.

Ainsi, après l'évolution complète, chacune des parties supérieure ou inférieure de la section réelle du cylindre

$$x^2+y^2=r^2$$

et de l'ellipsoïde

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}=1$$

sera revenue occuper sa position primitive.

Faisons maintenant varier $h$ entre $+b\sqrt{\frac{a}{a+b}}$ et $+b$ :

$x=\sqrt{r^2-h^2}$ sera encore, comme dans le cas précédent, réel, ou

imaginaire sans partie réelle, lorsque $\rho'$ ou $\rho$ passeront par zéro, tandis que, dans tout autre cas, il se composera d'une partie réelle et d'une partie imaginaire.

Au départ, c'est-à-dire lorsque, $\rho'$ étant nul, $\rho$ aura la valeur $+\sqrt{ab}$, $x$ sera réel et par exemple positif, et $z$ imaginaire sans partie réelle. Le point $[x, z]$ se trouvera alors sur la conjuguée $\frac{\beta''}{\beta} = \infty$ de l'ellipse réelle

$$\frac{x^2}{a^2} + \frac{z^2}{c^2} = 1 - \frac{h^2}{b^2};$$

supposons qu'il appartienne à la branche supérieure de cette conjuguée, ou que le point $[x, y, z]$ appartienne à la nappe supérieure de l'hyperboloïde

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1,$$

le coefficient de $\sqrt{-1}$ dans la valeur initiale de $z$ étant ainsi positif.

Comme au départ la caractéristique du point $[x, z]$ se trouvait infinie, nous devons, avant tout, nous demander quel signe elle aura pris immédiatement après.

Or l'équation

$$xdx = rdr,$$

dans laquelle il faudrait faire

$$x = +\sqrt{ab - h^2}, \quad r = +\sqrt{ab} \quad \text{et} \quad dr = d\rho + d\rho'\sqrt{-1},$$

donne

$$d\beta\sqrt{ab - h^2} = d\rho'\sqrt{ab},$$

c'est-à-dire que $d\beta$ sera d'abord positif; et comme $\beta''$ était déjà positif et avait une valeur finie, la caractéristique du point $[x, z]$ commencera par être positive.

Ainsi le point de contact, avec l'ellipse, de la conjuguée sur laquelle se transportera d'abord le point $[x, z]$, se trouvera dans le quatrième quadrant.

Au reste le point $[x, z]$ ne pourra jamais passer sur l'ellipse réelle

$$\frac{x^2}{a^2} + \frac{z^2}{c^2} = 1 - \frac{h^2}{b^2},$$

puisque toutes les fois que $x$ reprendra l'une de ses valeurs réelles

$$\pm \sqrt{ab - h^2}$$

correspondantes à $\rho' = 0$, $z$ en même temps reprendra l'une de ses valeurs imaginaires sans partie réelle

$$\frac{z}{c} = \pm \sqrt{1 - \frac{h^2}{b^2} - \frac{ab - h^2}{a^2}},$$

il restera donc toujours sur la même branche de la conjuguée qui le contiendra, ou plutôt il suivra cette branche de conjuguée dans son évolution autour de l'ellipse.

Il ne s'agit donc que de savoir par quelles valeurs passera la caractéristique de cette conjuguée.

Lorsque $\rho'$ atteindra sa valeur $+\sqrt{ab}$ et que par conséquent $\rho$ se trouvera nul, $x$ aura l'une des valeurs

$$x = \pm \sqrt{h^2 + ab}\sqrt{-1};$$

mais comme la partie imaginaire de $x$ a commencé par être positive et qu'elle ne s'est pas encore annulée, elle sera restée positive; de sorte que la seule valeur admissible pour $x$ sera

$$x = + \sqrt{h^2 + ab}\sqrt{-1}.$$

Quant à $z$, il aura l'une des valeurs

$$\frac{z}{c} = \pm \sqrt{1 - \frac{h^2}{b^2} + \frac{h^2 + ab}{b^2}},$$

qui sont réelles, car la condition

$$1 + \frac{h^2 + ab}{a^2} > \frac{h^2}{b^2}$$

revient à

$$ab^2 > h^2(a-b)$$

qui est satisfaite dans l'hypothèse où nous raisonnons, puisque $h$ est moindre que $b$.

Mais la partie réelle de $z$ un peu après le départ était négative, et elle n'est pas encore devenue nulle; elle a donc dû rester négative, par conséquent la valeur de $z$ doit être

$$\frac{z}{c} = -\sqrt{1 - \frac{h^2}{b^2} + \frac{h^2+ab}{a^2}};$$

le point $[x, z]$ se trouve donc alors sur la partie droite de la branche inférieure de la conjuguée $\frac{\beta''}{\beta} = 0$ de l'ellipse

$$\frac{x^2}{a^2} + \frac{z^2}{c^2} = 1 - \frac{h^2}{b^2}.$$

Aussitôt après, la caractéristique du point mobile changera de signe; en effet la différentielle de $x$ sera déterminée par l'équation

$$xdx = rdr$$

ou

$$\sqrt{-1}\sqrt{h^2+ab}\,(d\alpha + d\beta\sqrt{-1}) = \sqrt{-1}\sqrt{ab}\,(d\rho + d\rho'\sqrt{-1}),$$

c'est-à-dire

$$d\alpha\sqrt{h^2+ab} = d\rho\sqrt{ab}$$

et

$$d\beta\sqrt{a^2+ab} = d\rho'\sqrt{ab},$$

tandis que celle de $z$ le sera par l'équation

$$\frac{x\,dx}{a^2} + \frac{z\,dz}{c^2} = 0$$

ou

$$\frac{\sqrt{-1}\sqrt{h^2+ab}\,(d\alpha + d\beta\sqrt{-1})}{a^2} - \frac{\sqrt{1 - \frac{h^2}{b^2} + \frac{h^2+ab}{a^2}}}{c}(d\alpha'' + d\beta''\sqrt{-1}) = 0,$$

c'est-à dire

$$\frac{d\alpha\sqrt{h^2+ab}}{a^2} - \frac{d\beta''\sqrt{1-\frac{h^2}{b^2}+\frac{h^2+ab}{a^2}}}{c} = 0$$

et

$$\frac{d\beta\sqrt{a^2+ab}}{a^2} + \frac{d\alpha''\sqrt{1-\frac{h^2}{b^2}+\frac{h^2+ab}{a^2}}}{c} = 0.$$

Or $d\rho'$ étant négatif ainsi que $d\rho$, $d\alpha$, $d\beta$ et $d\beta''$ sont aussi négatifs, de sorte que $\beta$ qui était fini et positif, restant positif, la caractéristique devient négative, c'est-à-dire que le point $[x, z]$ se transporte sur la partie de droite de la branche de conjuguée de l'ellipse

$$\frac{x^2}{a^2} + \frac{z^2}{c^2} = 1 - \frac{h^2}{b^2}$$

qui la touche dans le troisième quadrant.

Il en résulte que lorsque $\rho'$ redeviendra nul, $\rho$ ayant alors la valeur $-\sqrt{ab}$, le point $[x, z]$ viendra se placer sur la partie inférieure de la branche de gauche de la conjuguée $\frac{\beta''}{\beta} = 0$ de l'ellipse

$$\frac{x^2}{a^2} + \frac{z^2}{c^2} = 1 - \frac{h^2}{b^2}.$$

Le mouvement se continuera ensuite évidemment dans le même sens; et lorsque $\rho$ et $\rho'$ seront revenus à leurs valeurs initiales, le point $[x, z]$ sera revenu aussi à sa position initiale.

Ainsi les deux portions supérieure et inférieure de la courbe que nous étudions, dans l'intervalle compris entre les plans

$$y = b\sqrt{\frac{a}{a+b}} \quad \text{et} \quad y = b,$$

après l'évolution complète, reprennent aussi leurs positions primitives.

Supposons enfin que $h$ dépasse la limite $b$. Le point $[x, z]$, alors, se

déplacera sur les conjuguées de l'ellipse imaginaire

$$\frac{x^2}{a^2}+\frac{z^2}{c^2}=-\left(\frac{h^2}{b^2}-1\right);$$

$x=\sqrt{r^2-h^2}$ pourra ou non devenir réel, en même temps que $r$, selon que $h^2$ sera moindre que $ab$, ou plus grand. Selon le cas, le point $[x, z]$ pourra donc ou non passer sur la conjuguée $\frac{\beta''}{\beta}=\infty$ du lieu.

La discussion, au reste, dans chacun des deux cas $h^2 < ab$ et $h^2 > ab$, s'achèverait comme précédemment, et il est inutile que nous insistions davantage.

**126**. Nous avons, dans ce qui vient d'être dit, supposé toujours que $\rho$ et $\rho'$ achevassent complétement leur évolution, mais la discussion a été dirigée de telle manière, que si l'on voulait s'arrêter à des valeurs correspondantes quelconques de $\rho$ et de $\rho'$, on pût immédiatement assigner la place que serait venue occuper la branche mobile de la courbe considérée.

**127**. *De la marche des valeurs d'une fonction de deux variables assujetties à une seule condition.* — Il suffirait évidemment de supprimer, dans l'exemple précédent, la condition

$$\beta'=0,$$

pour en former un qui se rapportât à la question présente.

Les équations

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}=1,$$

$$x^2+y^2=r^2,$$

$$r=\rho+\rho'\sqrt{-1},$$

$$\rho^2+\rho'^2=ab$$

détermineraient une surface variable de forme et de position avec la valeur de $\rho$; de sorte que la valeur initiale de $\rho$ étant par exemple

$+\sqrt{ab}$, il s'agirait de savoir ce qu'une nappe désignée de cette surface initiale serait devenue lorsque $\rho$ et $\rho'$ auraient achevé leur évolution.

Or la surface mobile contiendra toujours la courbe mobile dont nous avons étudié le mouvement dans le numéro précédent; on peut donc dire que la position finale de la nappe considérée de cette surface sera déterminée par la position finale de la branche correspondante de la courbe mobile.

*De la convergence du développement, par la formule de Taylor, d'une fonction de deux variables.*

**128.** $x_0$ et $y_0$ désignant les valeurs initiales des deux variables indépendantes $x$ et $y$, et $z_0$ celle de la fonction $z$, cette fonction est représentée jusqu'à un certain point par

$$\begin{aligned} z = z_0 &+ \left(\frac{dz}{dx}\right)_0 \frac{x-x_0}{1} + \left(\frac{d^2z}{dx^2}\right)_0 \frac{(x-x_0)^2}{1.2} + \dots \\ &+ \left(\frac{dz}{dy}\right)_0 \frac{y-y_0}{1} + 2\left(\frac{d^2z}{dx\,dy}\right)_0 \frac{(x-x_0)(y-y_0)}{1.2} + \dots \\ &+ \left(\frac{d^2z}{dy^2}\right)_0 \frac{(y-y_0)^2}{1.2} + \dots. \end{aligned}$$

Cette suite, comme étant indéfinie, constitue bien une série, si l'on prend le mot dans son acception la plus large, mais en réalité elle en fournira autant qu'on voudra imaginer de modes d'en grouper les termes : et non-seulement les conditions de convergence de toutes ces séries ne seraient pas identiques, mais même elles ne porteraient pas sur les mêmes groupes de coefficients différentiels.

Ainsi on pourrait regarder le développement comme représentant la somme des valeurs des séries formulées dans les diverses lignes horizontales; on pourrait grouper les termes suivant les lignes diagonales, etc.

Dans chaque cas, la condition de convergence dépendrait du mode de groupement des termes.

Il est donc indispensable de poser avant tout la question qu'on a en vue et de définir la série dont la convergence est mise en question.

Nous nous proposons ici de ramener la question de la convergence du développement d'une fonction de deux variables à celle de la convergence du développement d'une fonction d'une seule variable; le but indiqué désigne alors clairement la série dont il doit être question.

Nous nous occuperons exclusivement de la série formée des sommes de termes homogènes, par rapport à $(x - x_0)$ et à $(y - y_0)$, dans le développement général.

**129.** $x_0$ et $y_0$ étant toujours supposés connus, au lieu de nous donner $x$ et $y$, c'est-à-dire $(x - x_0)$ et $(y - y_0)$, nous nous donnerons $(x - x_0)$ et $\frac{y - y_0}{x - x_0}$, ce qui reviendra au même.

La fonction $z$, alors, dépendra de $x$ et du rapport $\frac{y - y_0}{x - x_0}$, que nous désignerons par $k$, de sorte que si l'équation, qui d'abord définissait $z$, était

$$f(x, y, z) = 0,$$

la nouvelle sera

$$f[x_0 + x - x_0, y_0 + k(x - x_0), z] = 0,$$

et nous développerons $z$ suivant les puissances croissantes de $(x - x_0)$, par la formule de Maclaurin, comme une fonction d'une seule variable.

Le développement de $z$ contiendra bien toujours deux variables $x$ et $k$, mais nous nous bornerons, d'abord, à déterminer, pour chaque valeur de $k$, la limite que ne devrait pas dépasser le module de $(x - x_0)$, pour que la série restât convergente.

En procédant ainsi nous n'aurons pas seulement obtenu les réponses propres à toutes les questions que pourrait comporter l'étude de la série, dans tous les cas où les valeurs finales des deux variables indépendantes seraient données à l'avance : nous aurons encore établi des bases pour résoudre, dans un grand nombre de cas, la question inverse où il s'agirait de déterminer la relation d'inégalité à laquelle devraient

satisfaire les modules de $(x - x_0)$ et de $(y - y_0)$ pour que la série restât convergente.

**150.** Le développement de $z$, ordonné suivant les puissances croissantes de $(x - x_0)$, est

$$z = z_0 + \left. \begin{array}{l} \left(\frac{dz}{dx}\right)_0 \\ + k\left(\frac{dz}{dy}\right)_0 \end{array} \right| \frac{x - x_0}{1} + \left. \begin{array}{l} \left(\frac{d^2 z}{dx^2}\right)_0 \\ + 2k\left(\frac{d^2 z}{dx\,dy}\right)_0 \\ + k^2\left(\frac{d^2 z}{dy^2}\right)_0 \end{array} \right| \frac{(x - x_0)^2}{1.2} + \ldots$$

Or, pour chaque valeur de $k$, la condition de convergence ne dépendra plus que de la nature du lieu

$$f[x, y_0 + k(x - x_0), z] = 0,$$

et de la place occupée sur ce lieu par le point $[x_0, z_0]$. La question sera donc entièrement identique à celle que nous avons traitée dans le chapitre VII.

**151.** Les points du lieu

$$f[x, y_0 + k(x - x_0), z] = 0$$

où le développement de $z$ peut être arrêté, sont ceux où les dérivées de $z$ par rapport à $x$ deviennent infinies à partir d'un certain ordre. Mais nous ne pouvons prétendre ici à distinguer tous les cas les uns des autres : nous nous bornerons donc à l'examen de celui où les dérivées d'ordres supérieurs ne sauraient devenir infinies qu'avec et après celle du premier ordre.

La dérivée de $z$ par rapport à $x$ en un point du lieu

$$f[x, y_0 + k(x - x_0), z] = 0$$

est

$$-\frac{\frac{df}{dx}+k\frac{df}{dy}}{\frac{df}{dz}},$$

$y$ désignant la variable $x_0 + k(x - x)$; les points dangereux seront donc fournis par les équations

$$f'_z[x, y_0 + k(x - x_0), z] = 0$$

et

$$f[x, y_0 + k(x - x_0), z] = 0.$$

Ces points appartiennent à la courbe de contact de la surface

$$f(x, y, z) = 0$$

avec le cylindre qui lui serait circonscrit parallèlement aux $z$, car cette courbe aurait pour équations

$$f'_z(x, y, z) = 0$$

et

$$f(x, y, z) = 0$$

où il suffirait de faire $y = y_0 + k(x - x_0)$ pour retrouver les précédentes.

Ainsi les points dangereux du lieu

$$f[x_0, y_0 + k(x - x_0), z] = 0$$

sont les points d'intersection du plan réel ou imaginaire

$$y = y_0 + k(x - x_0)$$

avec la courbe de contact dont nous parlons.

Si la projection sur le plan des $xy$ de cette courbe est représentée par

$$\varphi(x, y) = 0,$$

les abscisses des points dangereux du lieu

$$f[x, y_0 + k(x - x_0), z] = 0$$

seront donc fournies par les équations

$$\varphi(x, y) = 0,$$
$$y = y_0 + k(x - x_0),$$

c'est-à-dire que les projections de ces points sur le plan des $xy$ seront les intersections du contour apparent

$$\varphi(x, y) = 0$$

et de la droite

$$y = y_0 + k(x - x_0),$$

si, bien entendu, dans cet énoncé, par contour apparent de la surface on entend le contour apparent réel et toutes ses conjuguées.

**132.** La constante $k$ marque la direction du chemin qui conduirait du point $[x_0, y_0]$ au point $[x, y]$, et il est évident que le module de la différence entre $x_0$ et l'abscisse du point dangereux où s'arrêtera le développement dépendra essentiellement de $k$; ainsi le module maximum de la différence $x - x_0$ et par suite celui de $y - y_0$, seront essentiellement variables et intimement liés à la valeur de $k$.

Cela est tellement vrai, que la direction $k$ pourrait être telle, que les modules de

$$x_0 - X \quad \text{et de} \quad y_0 - Y$$

pussent devenir infinis sans que la série cessât de rester convergente.

Il suffirait en effet pour cela que la droite

$$y = y_0 + k(x - x_0$$

coïncidât avec une asymptote réelle ou imaginaire du lieu

$$\varphi(x, y) = 0$$

qui ne rencontrât celui-ci nulle part ailleurs qu'à l'infini.

En voici un exemple :

Soit l'équation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1,$$

qui donne

$$\frac{z}{c} = \sqrt{1 - \frac{x^2}{a^2} - \frac{y^2}{b^2}};$$

si

$$\frac{y_0}{x_0} = \frac{b}{a}\sqrt{-1},$$

et que l'on pose d'ailleurs

$$\frac{y - y_0}{x - x_0} = \frac{b}{a}\sqrt{-1},$$

le point mobile $[x, y]$ décrira une asymptote du contour apparent

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - 1 = 0$$

de la surface, asymptote qui ne rencontrera ce contour nulle part ailleurs qu'à l'infini, $z$ devra donc alors se développer en série convergente quel que soit le module de $x - x_0$.

Et en effet dans ce cas $z$ ne sera qu'une constante $c$; toutes les sommes de termes homogènes du développement

$$\begin{aligned} z_0 &+ \left(\frac{dz}{dx}\right)_0 (x - x_0) + \ldots \\ &+ \left(\frac{dz}{dy}\right)_0 (y - y_0) + \ldots \\ &+ \ldots \end{aligned}$$

seront donc nulles d'elles-mêmes; les modules de $(x - x_0)$ et de $(y - y_0)$ pourraient donc être infinis, que la série, définie comme nous l'avons définie, n'en resterait pas moins convergente.

On voit par là combien il était contraire à la réalité des choses, de supposer, comme on l'a fait, avant tout examen, que les modules de $(x - x_0)$ et de $(y - y_0)$ fussent indépendants et eussent des maxima respectifs fixes.

## NOTE.

Je n'avais pas connaissance, lorsque j'écrivais le chapitre VII de mon Mémoire, d'une Note fort courte, mais très-importante, que M. Tchebicheff a insérée en 1844 dans le *Journal de Crelle* (t. XXVIII, pages 279 à 283).

Cette *Note sur la convergence de la série de Taylor* contient à certains égards la bonne solution de la question.

Le dernier énoncé, fourni à cette époque par M. Cauchy, de la condition de convergence, était ainsi conçu :

« $x$ désignant une variable réelle ou imaginaire, une fonction réelle ou imaginaire » de $x$ sera développable en série convergente ordonnée suivant les puissances » ascendantes de $x$, tant que le module de $x$ conservera une valeur inférieure » à la plus petite de celles pour lesquelles la fonction ou sa dérivée cesse d'être finie » et continue. »

M. Tchebicheff propose de dire :

« La série de Taylor

$$f(a) + \frac{z}{1} f'(a) + \frac{z^2}{1 \cdot 2} f''(a) + \ldots$$

» est divergente ou convergente suivant que le module de $z$ est plus grand ou plus » petit que celui de la valeur imaginaire $r$ qui rendrait infinie ou discontinue une des » fonctions

$$f(a + x),\ f'(a + x),\ f''(a + x) \ldots \text{»}$$

En supprimant de cet énoncé l'assertion que la série deviendrait divergente au delà du premier point dangereux, on trouve la règle que j'ai proposée moi-même et dont je croyais la formule nouvelle.

Les deux énoncés de M. Tchebicheff et de M. Lamarle sont vicieux, il est vrai, sous un rapport, mais tous ceux qu'on a donnés depuis sont entachés du même défaut; au

contraire, ce qu'ils contenaient de rigoureusement exact a été compliqué depuis de conditions qui n'ont, ni de près, ni de loin, le moindre rapport à la convergence de la série.

Même on en est venu jusqu'à ne plus caractériser les points, où le développement peut être arrêté, que par la seule qualité commune, qui, justement, n'apporte par elle-même aucun obstacle au développement.

Car s'il faut bien, il est vrai, qu'un point soit multiple pour être dangereux, ce n'est en aucune façon comme point multiple qu'il est dangereux, mais parce que, suivant M. Tchebicheff, les dérivées de la fonction y deviennent infinies, à partir d'un certain ordre, ou, suivant M. Lamarle, parce que les valeurs de la fonction peuvent se permuter autour de ce point.

Pour qu'on ait cru devoir changer les énoncés proposés par M. Tchebicheff et par M. Lamarle, il faut qu'ils n'aient été bien compris ni l'un ni l'autre.

C'est pourquoi je pense qu'il ne sera pas inutile de revenir sur la démonstration de leur entière identité, démonstration que je n'ai qu'indiquée dans le chapitre VII.

Ce qui est en question est de savoir si les valeurs de la fonction $y$, qui diffèrent infiniment peu de l'ordonnée d'un point multiple du lieu $f(x,y) = 0$, peuvent se permuter entre elles, la variable $x$ ne prenant elle-même que des valeurs infiniment voisines de l'abscisse de ce point multiple, sans qu'aucune des dérivées de la fonction, quel qu'en soit d'ailleurs l'ordre, soit infinie en ce point.

Il me semble qu'il suffit pour cela d'observer que pour que deux valeurs de $y$ se permutent, il faut que toutes leurs dérivées se permutent aussi. Cette remarque est bien concluante en effet; car, de même qu'on ne saurait admettre que deux valeurs de $y$, correspondantes à une même abscisse, mais séparées par un intervalle fini, se permutassent sans que la variable $x$ se fût écartée de sa valeur initiale d'une quantité finie, on n'admettra pas davantage que les dérivées d'ordres supérieurs à celui où a lieu la séparation définitive, se permutent, sans cette condition; or si elles ne peuvent se permuter, les valeurs de la fonction ne se permuteront pas non plus.

On peut pousser plus loin cette analyse :

Si en un point multiple du lieu $f(x,y) = 0$ quelques dérivées, d'ordre $n$, se séparent des autres, en prenant d'ailleurs des valeurs distinctes, ces dérivées ne pouvant se permuter, ni entre elles, ni avec les autres, dans un parcours infiniment petit de la variable, il en sera de même des formes correspondantes de la fonction.

En second lieu si, parmi les dérivées d'ordre $n'$, on en trouve plusieurs ayant une même valeur $k$, d'autres ayant une même valeur $k'$, etc., évidemment, sans pouvoir encore rien affirmer de la permutabilité ou de l'impermutabilité entre elles, de celles des dérivées qui, pour une valeur de $x$ infiniment voisine de l'abscisse du point multiple, prennent des valeurs infiniment peu différentes de $k$, on pourra du moins affirmer qu'elles ne se permuteront pas avec les autres, et par suite conclure dans le même sens et avec les mêmes restrictions pour les formes correspondantes de la fonction.

Enfin, si quelques dérivées de la fonction restent confondues jusqu'à l'ordre $n''$, et qu'au lieu de se séparer à l'ordre $n''+1$ elles y deviennent toutes infinies, les formes

correspondantes de la fonction seront permutables entre elles, mais non avec les autres.

Ainsi les formes de la fonction, qui peuvent se permuter entre elles, autour d'un point multiple, sont celles dont les dérivées deviennent infinies au même ordre, après être restées confondues jusqu'à l'ordre précédent.

Ce sont là sans doute les groupes circulaires que le calcul direct avait révélés à M. Puiseux; en les définissant comme on vient de le faire, il devient superflu de les déterminer à l'avance. Que l'équation soit d'ailleurs algébrique ou transcendante, on les retrouvera toujours sans difficulté.

Je dois, en terminant cette troisième partie, signaler une erreur contenue au chapitre III.

Lorsque j'écrivais ce chapitre, je croyais que l'enveloppe imaginaire des conjuguées aurait habituellement les parties réelles de ses coordonnées constantes; et j'en concluais que l'évaluation approximative de l'intégrale $\int ydx$ prise le long de cette enveloppe pourrait se faire, *dans le plus grand nombre des cas*, par la quadrature approchée de l'enveloppe.

J'avais évidemment pris l'exception pour la règle générale.

Quant aux raisons que je donnais à l'appui de mon opinion, elles sont aussi mauvaises que possible; mais je n'aurais pas cru devoir en parler, si je n'avais eu à faire une rectification plus importante

# THÉORÈME

CONCERNANT

## LE PRODUIT DE DEUX NOMBRES PREMIERS ÉGAUX OU INÉGAUX DE LA FORME $8\mu+3$;

**Par M. J. LIOUVILLE.**

---

Dans le cahier d'août 1860, nous nous sommes occupés du produit de deux nombres premiers, l'un de la forme $16k+3$, l'autre de la forme $16h+5$. C'était un premier pas dans une voie qui sera féconde. Nous allons donner dans cet article et dans les suivants d'autres propositions du même genre. Il nous semble que ces théorèmes concernant un produit de deux nombres premiers n'offrent pas moins d'intérêt que ceux qui se rapportent aux nombres premiers pris isolément.

Soient $a$ et $b$ deux nombres premiers, égaux ou inégaux, mais tous deux $\equiv 3 \pmod{8}$. Le produit $ab$, que je représenterai par $m$, jouira d'une propriété dont nous voulons dire ici deux mots.

Cette propriété consiste en ce que, pour chaque produit $m$, on peut poser au moins une fois, et toujours un nombre impair de fois, l'équation

$$m = 4x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs, et $p$ un nombre premier qui ne divise pas $y$. Nous admettons pour $l$ la valeur zéro. Quant au nombre premier $p$, nous ne le soumettons à priori à aucune condition, mais vu la forme donnée des facteurs $a$ et $b$ de $m$, et $x$, $y$ étant impairs, il est évident qu'il ne pourra être que de la forme $8g+5$.

En supposant égal à 3 un des deux nombres premiers $a$, $b$ dont $m$ est le produit, on retomberait sur un théorème que nous avons donné

déjà (cahier de décembre 1860). Dans les exemples qui vont suivre, nous avons donc pris $a$ et $b > 3$.

*Premier exemple :* $a = 11$, $b = 11$, $m = 121$. — Notre théorème se trouve vérifié, eu égard à l'équation canonique

$$121 = 4.1^2 + 13.3^2.$$

*Deuxième exemple :* $a = 11$, $b = 19$, $m = 209$. — Notre théorème est encore vérifié, mais il y a cette fois trois équations canoniques, savoir

$$209 = 4.3^2 + 173.1^2,$$
$$209 = 4.5^2 + 109.1^2,$$
$$209 = 4.7^2 + 13.1^2.$$

*Troisième exemple :* $a = 19$, $b = 19$, $m = 361$. — Même vérification, et les trois équations canoniques ci-après :

$$361 = 4.3^2 + 13.5^2,$$
$$361 = 4.5^2 + 29.3^2,$$
$$361 = 4.9^2 + 37.1^2.$$

On prolongera aisément, si on le désire, ces exercices numériques : partout, notre théorème aura lieu.

# THÉORÈME

CONCERNANT

## LE PRODUIT DE DEUX NOMBRES PREMIERS, L'UN DE LA FORME $8\mu+1$, L'AUTRE DE LA FORME $8\nu+3$;

**Par M. J. LIOUVILLE.**

Soient $a$ et $b$ deux nombres premiers donnés, $a$ de la forme $8\mu+1$, $b$ de la forme $8\nu+3$. Considérons leur produit $ab$, que nous représenterons par $m$, et faisons de toutes les manières possibles

$$m = x^2 + 2p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs, et $p$ un nombre premier, de la forme $8g+5$, et non diviseur de $y$. On veut savoir à priori par une règle facile si le nombre N des décompositions de $m$ ainsi obtenues sera pair ou impair, zéro étant compté comme nombre pair.

Or $a$ étant un nombre premier $8\mu+1$, on peut poser d'une seule manière, en nombres entiers,

$$a = r^2 + 8s^2,$$

et je trouve que l'on a toujours $N \equiv s \pmod{2}$, en sorte que N est pair quand $s$ est pair, mais impair quand $s$ est impair.

Nous exigeons que $p$ soit de la forme $8g+5$. Cette condition pourrait être remplacée par une autre qui porterait sur $x$. En effet, le produit $m$ est toujours de la forme $8n+3$, mais tantôt $n$ est pair ($n=2k$), tantôt $n$ est impair ($n=2k+1$). Cela observé, on conclura aisément de l'équation

$$m = x^2 + 2p^{4l+1}y^2,$$

que pour que $p$ soit de la forme $8g+5$, il faut et il suffit que $x$ soit

de la forme $8t \pm 3$ quand $n$ est pair, et de la forme $8t \pm 1$ quand $n$ est impair. Ainsi, pour les produits $m$ de la forme $16k + 3$, on devra prendre pour $x^2$ les termes de la suite

$$3^2,\ 5^2,\ 11^2,\ 13^2, \ldots,$$

tandis que pour les produits $m$ de la forme $16k + 11$, les valeurs de $x^2$ à employer seront

$$1^2,\ 7^2,\ 9^2,\ 15^2, \ldots.$$

Pour

$$a = 17 = 3^2 + 8.1^2,$$

on a $s = 1$, donc N impair. Avec $a = 17$, soit d'abord $b = 3$, d'où le produit 17.3, ou 51, qui appartient à la forme $16k + 3$. On trouve pour ce produit (conformément à notre théorème) l'équation canonique

$$51 = 5^2 + 2.13.1^2.$$

Soit ensuite $b = 11$. Le produit 17.11, ou 187, appartiendra cette fois à la forme $16k + 11$, et l'on aura encore une seule équation canonique

$$187 = 9^2 + 2.53.1^2.$$

Pour

$$a = 41 = 3^2 + 8.2^2,$$

on a au contraire $s = 2$, donc N pair. Et en effet on trouve alors N égal à 2 pour $b = 3$, c'est-à-dire pour le produit 123, qui est de la forme $16k + 11$, et qui donne lieu aux équations canoniques

$$123 = 1^2 + 2.61.1^2, \quad 123 = 7^2 + 2.37.1^2.$$

# THÉORÈME

CONCERNANT

## LE PRODUIT DE DEUX NOMBRES PREMIERS ÉGAUX OU INÉGAUX DE LA FORME $24\mu + 5$;

**Par M. J. LIOUVILLE.**

Désignons par $m$ le produit de deux nombres premiers donnés, l'un et l'autre de la forme $24\mu + 5$, mais du reste égaux ou inégaux. On aura au sujet du produit $m$ ce théorème, que l'on peut poser au moins une fois, et toujours un nombre impair de fois, l'équation

$$m = 12x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs et $p$ un nombre premier qui ne divise pas $y$. On admet pour $l$ la valeur zéro. Quant au nombre premier $p$, nous ne lui imposons à priori aucune condition, mais il est évident qu'il ne peut qu'être $\equiv 5 \pmod{8}$ et $\equiv 1 \pmod{3}$ : il sera donc nécessairement de la forme $24g + 13$.

L'exemple le plus simple est celui de

$$m = 5.5,$$

ou de

$$m = 25.$$

Or on a l'équation canonique

$$25 = 12.1^2 + 13.1^2.$$

Soit ensuite

$$m = 5.29,$$

c'est-à-dire

$$m = 145.$$

On aura de même l'équation canonique

$$145 = 12.3^2 + 37.1^2.$$

On n'en a pas en retranchant 12 de 145, car le reste 133 qu'on obtient ainsi est le produit de 7 par 19.

Soit enfin

$$m = 29.29,$$

c'est-à-dire

$$m = 841.$$

Les équations canoniques seront alors au nombre de trois

$$841 = 12.1^2 + 829.1^2,$$
$$841 = 12.3^2 + 733.1^2,$$
$$841 = 12.5^2 + 541.1^2,$$

où 829, 733 et 541 sont des nombres premiers. On ne trouve pas d'équation canonique en retranchant $12.7^2$ de 841, car le reste 253 est le produit de 11 par 23. Ainsi, dans ce dernier exemple, comme dans ceux qui précèdent et dans tous ceux qu'on pourrait ajouter, notre théorème a lieu.

# THÉORÈME

CONCERNANT

LE PRODUIT DE DEUX NOMBRES PREMIERS ÉGAUX OU INÉGAUX DE LA FORME $24\mu + 7$;

PAR M. J. LIOUVILLE.

---

Le produit de deux nombres premiers égaux ou inégaux de la forme $24\mu + 7$ jouit d'une propriété toute semblable à celle que nous avons indiquée dans l'article précédent au sujet du produit de deux nombres premiers de la forme $24\mu + 5$.

*Théorème.* — « Pour chaque produit $m$ de deux nombres premiers, » égaux ou inégaux, mais tous deux $\equiv 7$ (mod. 24), on peut poser » au moins une fois, et toujours un nombre impair de fois, l'équation

$$m = 12x^2 + p^{4l+1}y^2,$$

» $x$ et $y$ étant des entiers impairs et $p$ un nombre premier qui ne » divise pas $y$. »

On admet pour $l$ la valeur zéro. Quant au nombre premier $p$, on ne lui impose à priori aucune condition; mais il est évident qu'il sera $\equiv 5$ (mod. 8) et $\equiv 1$ (mod. 3). On le trouvera donc toujours de la forme $24g + 13$.

L'exemple le plus simple est celui de

$$m = 7.7$$

ou de

$$m = 49.$$

Or on a l'équation canonique

$$49 = 12.1^2 + 37.1^2.$$

Soit ensuite

$$m = 7.31,$$

c'est-à-dire

$$m = 217.$$

On aura de même l'équation canonique

$$217 = 12.3^2 + 109.1^2.$$

On n'obtient pas d'équation canonique en retranchant 12 de 217, car le reste 205 est le produit de 5 par 41.

Soit enfin

$$m = 31.31,$$

c'est-à-dire

$$m = 961;$$

et cette fois encore notre théorème sera vérifié, les équations canoniques étant au nombre de trois, savoir :

$$961 = 12.3^2 + 853.1^2,$$
$$961 = 12.5^2 + 661.1^2,$$
$$961 = 12.7^2 + 373.1^2,$$

où 853, 661, 373 sont des nombres premiers. On n'obtient pas d'équation canonique en retranchant 12 de 961; car le reste 949 est le produit des deux nombres premiers 13 et 73.

# THÉORÈME

CONCERNANT

LE PRODUIT DE DEUX NOMBRES PREMIERS, L'UN DE LA FORME $40\mu+3$, L'AUTRE DE LA FORME $40\nu+7$;

PAR M. J. LIOUVILLE.

Désignons par $m$ le produit de deux nombres premiers donnés, l'un de la forme $40\mu+3$, l'autre de la forme $40\nu+7$. On aura au sujet du produit $m$ ce théorème, que l'on peut poser au moins une fois, et toujours un nombre impair de fois, l'équation

$$m = 10x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs, et $p$ un nombre premier qui ne divise pas $y$. On admet pour $l$ la valeur zéro. Quant au nombre premier $p$, nous ne lui imposons à priori aucune condition; mais il est évident que notre équation

$$m = 10x^2 + p^{4l+1}y^2$$

ne pourrait pas être vérifiée, si l'on n'avait pas à la fois

$$p \equiv 3 \pmod{8}$$

et

$$p \equiv \pm 1 \pmod{5}.$$

Ainsi $p$ sera de l'une ou de l'autre des deux formes

$$40g+11, \quad 40g+19.$$

L'exemple le plus simple est celui de

$$m = 3.7,$$

c'est-à-dire de

$$m = 21.$$

Or on a l'équation canonique

$$21 = 10.1^2 + 11.1^2.$$

Vient ensuite

$$m = 3.47,$$

c'est-à-dire

$$m = 141,$$

et cette fois encore on a une seule équation canonique, savoir

$$141 = 10.1^2 + 131.1^2:$$

on n'obtient pas une telle équation en retranchant $10.3^2$ de 141, car le reste 51 est le produit de 3 par 17.

Soit enfin

$$m = 7.43,$$

c'est-à-dire

$$m = 301,$$

et notre théorème sera également vérifié, grâce à l'équation canonique

$$301 = 10.3^2 + 211.1^2.$$

Les restes 291 et 51 obtenus en retranchant 10 et $10.5^2$ de 301 n'ont pas la forme voulue; 291 est le produit des deux nombres premiers 3 et 97.

Nous ne voyons pas qu'il y ait intérêt à pousser plus loin ces vérifications numériques.

# THÉORÈME

CONCERNANT

LE PRODUIT DE DEUX NOMBRES PREMIERS, L'UN DE LA FORME $40\mu + 7$, L'AUTRE DE LA FORME $40\nu + 27$;

PAR M. J. LIOUVILLE.

Désignons par $m$ le produit de deux nombres premiers donnés, l'un de la forme

$$40\mu + 7,$$

l'autre de la forme

$$40\nu + 27.$$

On aura au sujet du produit $m$ ce théorème, que l'on peut poser au moins une fois, et toujours un nombre impair de fois, l'équation

$$m = 10x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs et $p$ un nombre premier qui ne divise pas $y$. On admet pour $l$ la valeur zéro. Quant au nombre premier $p$, nous ne lui imposons à priori aucune condition; mais avec la nature indiquée du nombre $m$, et $x$ étant impair, il est évident que notre équation

$$m = 10x^2 + p^{4l+1}y^2$$

entraînera les deux congruences

$$p \equiv 3 \pmod{8}$$

et

$$p \equiv \pm 1 \pmod{5}.$$

On peut donc affirmer que $p$ sera toujours de l'une ou de l'autre des

deux formes

$$40g + 11, \quad 40g + 19.$$

Nous nous contenterons de vérifier notre théorème sur un seul exemple, en faisant

$$m = 7.67,$$

c'est-à-dire

$$m = 469,$$

et nous le trouverons en effet confirmé par l'équation canonique

$$469 = 10.3^2 + 379.1^2,$$

où 379 est un nombre premier. On n'obtient pas d'équation canonique en retranchant $10.1^2$, ni $10.5^2$, de 469; car des deux restes 459 et 219 qui s'offrent alors, l'un est le produit du cube de 3 par 17, et l'autre est le produit de 3 par 73.

En allant plus loin, on trouverait pour $m$ de grands nombres qui rendent les vérifications pénibles; mais l'exactitude de notre théoreme ne dépend pas de ces calculs.

Avons-nous besoin de faire observer que ce théorème devra être rapproché de celui qu'on a donné dans l'article précedent? On en trouvera deux autres d'un genre semblable dans les articles ci-apres.

# THÉORÈME

CONCERNANT

## LE PRODUIT DE DEUX NOMBRES PREMIERS, L'UN DE LA FORME $40\mu + 3$, L'AUTRE DE LA FORME $40\nu + 23$;

PAR M. J. LIOUVILLE.

Désignons par $m$ le produit de deux nombres premiers donnés, l'un de la forme $40\mu + 3$, l'autre de la forme $40\nu + 23$. Nous aurons au sujet du produit $m$ ce théorème, que l'on peut poser au moins une fois, et toujours un nombre impair de fois, l'équation

$$m = 10x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs, et $p$ un nombre premier qui ne divise pas $y$. On admet pour $l$ la valeur zéro. Quant au nombre premier $p$, nous ne le soumettons à priori à aucune condition ; mais avec la valeur que nous attribuons à $m$, et $x$ étant impair, il est évident que l'équation

$$m = 10x^2 + p^{4l+1}y^2$$

entraîne ces deux congruences

$$p \equiv 3 \pmod{8},$$

et

$$p \equiv \pm 1 \pmod{5}.$$

On peut dès lors affirmer que $p$ sera de l'une ou de l'autre des deux formes

$$40g + 11, \quad 40g + 19.$$

Contentons-nous de vérifier notre théorème sur des exemples très-simples.

*Premier exemple :* $m = 3.23$, c'est-à-dire $m = 69$. — On a l'équation canonique

$$69 = 10.1^2 + 59.1^2.$$

*Deuxième exemple :* $m = 3.103$, c'est-à-dire $m = 309$. — On a l'équation canonique

$$309 = 10.5^2 + 59.1^2.$$

On n'a pas d'équation canonique en retranchant 10 ni $10.3^2$ de 309, les restes 299 et 219 étant respectivement égaux à 13.23 et 3.73.

*Troisième exemple :* $m = 3.223$, c'est-à-dire $m = 669$. — Les équations canoniques sont alors au nombre de trois, savoir

$$669 = 10.1^2 + 659.1^2,$$
$$669 = 10.5^2 + 419.1^2,$$
$$669 = 10.7^2 + 179.1^2.$$

On n'a pas d'équation canonique en retranchant $10.3^2$ de 669, puisque le reste 579 est le produit de deux nombres premiers 3 et 193.

*Quatrième exemple :* $m = 43.23$, c'est-à-dire $m = 989$. — Cette fois encore il y a trois équations canoniques :

$$989 = 10.5^2 + 739.1^2,$$
$$989 = 10.7^2 + 499.1^2,$$
$$989 = 10.9^2 + 179.1^2.$$

On n'a pas d'équation canonique en retranchant $10.1^2$ ni $10.3^2$ de 989 ; car les deux restes 979 et 899, qu'on obtient ainsi, sont égaux respectivement à 11.89 et 29.31.

Ces exemples suffiront, je crois ; mais si loin qu'on veuille aller dans les exercices numériques, on trouvera toujours notre théorème exact.

# THÉORÈME

CONCERNANT

## LE PRODUIT DE DEUX NOMBRES PREMIERS, L'UN DE LA FORME $40\mu + 23$, L'AUTRE DE LA FORME $40\nu + 27$;

**Par M. J. LIOUVILLE.**

---

Soient $a$ et $b$ deux nombres premiers donnés, l'un de la forme

$$40\mu + 23,$$

l'autre de la forme

$$40\nu + 27.$$

Désignons par $m$ leur produit $ab$. Nous aurons au sujet du produit $m$ ce théorème, que l'on peut poser au moins une fois, et toujours un nombre impair de fois, l'équation

$$m = 10x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs, et $p$ un nombre premier qui ne divise pas $y$. On admet pour $l$ la valeur zéro. Quant au nombre premier $p$, nous ne le soumettons à priori à aucune condition; mais avec la valeur indiquée pour $m$, et $x$ devant être un entier impair, il est évident que notre équation

$$m = 10x^2 + p^{4l+1}y^2$$

entraînera les deux congruences

$$p \equiv 3 \pmod{8}$$

et

$$p \equiv \pm 1 \pmod{5}.$$

Il sera donc de l'une ou de l'autre des deux formes

$$40g + 11, \quad 40g + 19.$$

Nous nous contenterons d'un seul exemple, en faisant

$$a = 23, \quad b = 67,$$

d'où

$$m = 23.67,$$

c'est-à-dire

$$m = 1541,$$

et nous trouverons notre théorème confirmé par les cinq équations canoniques ci-après :

$$1541 = 10.1^2 + 1531.1^2,$$
$$1541 = 10.3^2 + 1451.1^2,$$
$$1541 = 10.5^2 + 1291.1^2,$$
$$1541 = 10.7^2 + 1051.1^2,$$
$$1541 = 10.11^2 + 331.1^2,$$

où

$$1531, \quad 1451, \quad 1291, \quad 1051, \quad 331$$

sont des nombres premiers. On n'a pas d'équation canonique en retranchant $10.9^2$ de $1541$, puisque le reste $731$ qu'on obtient ainsi est le produit de $17$ par $43$.

# THÉORÈME

CONCERNANT

## LE PRODUIT DE DEUX NOMBRES PREMIERS ÉGAUX OU INÉGAUX DE LA FORME $120\mu+31$;

PAR M. J. LIOUVILLE.

Désignons par $m$ le produit de deux nombres premiers donnés, l'un et l'autre de la forme $120\mu+31$, mais du reste égaux ou inégaux. On aura au sujet du produit $m$ ce théorème, que l'on peut poser au moins une fois, et toujours un nombre impair de fois, l'équation

$$m = 60x^2 + p^{4l+1}y^2,$$

$x$ et $y$ étant des entiers impairs, et $p$ un nombre premier qui ne divise pas $y$. On admet pour $l$ la valeur zéro. Quant au nombre premier $p$, nous ne lui imposons à priori aucune condition; mais il est évident que notre équation

$$m = 60x^2 + p^{4l+1}y^2$$

ne pourrait pas être vérifiée si l'on n'avait pas, à la fois,

$$p \equiv 5 \pmod{8}$$

et

$$p \equiv 1 \pmod{3}, \qquad p \equiv \pm 1 \pmod{5}.$$

On peut donc affirmer que $p$ sera toujours de l'une ou de l'autre des deux formes

$$120g + 61, \qquad 120g + 109.$$

Nous nous contenterons de vérifier notre théorème sur deux exem-

ples. Le plus simple est celui de

$$m = 31.31,$$

c'est-à-dire de

$$m = 961.$$

Or on a l'équation canonique

$$961 = 60.3^2 + 421.1^2.$$

On n'a pas d'équation canonique en retranchant 60 de 961, puisque le reste 901 est le produit de 17 par 53.

Soit ensuite

$$m = 151.31,$$

c'est-à-dire

$$m = 4681.$$

Les équations canoniques seront alors au nombre de trois, savoir

$$4681 = 60.1^2 + 4621.1^2,$$
$$4681 = 60.5^2 + 3181.1^2,$$
$$4681 = 60.7^2 + 1741.1^2,$$

où 4621, 3181, 1741 sont des nombres premiers. On n'a pas d'équation canonique en retranchant $60.3^2$ de 4681, puisque le reste 4141 est le produit de 41 par 101.

# THÉORÈME

CONCERNANT

## LE PRODUIT DE DEUX NOMBRES PREMIERS ÉGAUX OU INÉGAUX DE LA FORME $120\mu + 79$;

PAR M. J. LIOUVILLE.

Le produit de deux nombres premiers égaux ou inégaux de la forme $120\mu + 79$ jouit d'une propriété toute semblable à celle que nous avons indiquée dans l'article précédent au sujet du produit de deux nombres premiers de la forme $120\mu + 31$.

On a en effet la proposition suivante : « Pour chaque produit $m$ de » deux nombres premiers, égaux ou inégaux, mais tous les deux $\equiv 79$ » (mod. 120), on peut poser au moins une fois, et toujours un nombre » impair de fois, l'équation

$$m = 60x^2 + p^{4l+1}y^2,$$

» $x$ et $y$ étant des entiers impairs, et $p$ un nombre premier qui ne » divise pas $y$. »

On admet pour $l$ (comme d'ordinaire) la valeur zéro. Quant au nombre premier $p$, on ne lui impose à priori aucune condition ; mais il est évident qu'il devra vérifier les trois congruences

$$p \equiv 5 \pmod{8}$$

et

$$p \equiv 1 \pmod{3}, \qquad p \equiv \pm 1 \pmod{5}.$$

Il sera donc nécessairement de l'une ou de l'autre des deux formes

$$120g + 61, \quad 120g + 109.$$

Nous nous contenterons d'un seul exemple plus simple, celui de

$$m = 79 \cdot 79,$$

c'est-à-dire de

$$m = 6241,$$

pour lequel on a trois équations canoniques

$$6241 = 60.3^2 + 5701.1^2,$$
$$6241 = 60.7^2 + 3301.1^2,$$
$$6241 = 60.9^2 + 1381.1^2,$$

où 5701, 3301, 1381 sont des nombres premiers.

On n'a pas d'équation canonique en retranchant $60.1^2$, ni $60.5^2$, de 6241, car les restes 6181 et 4741 se décomposant en facteurs premiers de cette manière 7.883, 11.431, aucun d'eux n'a la forme exigée par notre énoncé.

# THÉORÈME

CONCERNANT

## LE PRODUIT DE DEUX NOMBRES PREMIERS, L'UN DE LA FORME $120\mu+31$, L'AUTRE DE LA FORME $120\nu+79$;

**Par M. J. LIOUVILLE.**

Ce théorème doit être joint à ceux que nous venons de donner au sujet du produit de deux nombres premiers de la forme $120\mu+31$ et de deux nombres premiers de la forme $120\mu+79$. On y emploie en effet des expressions du même genre.

*Théorème.* — « Pour chaque produit $m$ de deux nombres premiers, » l'un de la forme $120\mu+31$, l'autre de la forme $120\mu+79$, on peut » poser au moins une fois, et toujours un nombre impair de fois, l'é- » quation

$$m = 60x^2 + p^{4l+1}y^2,$$

» $x$ et $y$ étant des entiers impairs, et $p$ un nombre premier qui ne di- » vise pas $y$. »

Nous n'avons pas besoin d'avertir qu'on admet pour $l$ la valeur zéro. Quant au nombre premier $p$, que nous n'assujettissons à priori à aucune condition, on s'assurera sans peine qu'il ne peut être que de l'une ou de l'autre des deux formes

$$120\mu+61, \quad 120\mu+109.$$

Ici, en effet, comme dans les deux articles précédents, il devra vérifier les trois congruences

$$p \equiv 5 \pmod{8}$$

et

$$p \equiv 1 \pmod{3}, \qquad p \equiv \pm 1 \pmod{5},$$

qui sont une conséquence immédiate de l'équation même que nous posons.

Cette fois encore, nous nous bornerons à l'exemple le plus simple, en prenant

$$m = 31.79,$$

c'est-à-dire

$$m = 2449,$$

et notre théorème sera vérifié, vu l'équation canonique

$$2449 = 60.1^2 + 2389.1^2,$$

où 2389 est un nombre premier. On n'a pas d'équation canonique en retranchant $60.3^2$, ni $60.5^2$, de 2449; car les restes 1909 et 949 sont l'un et l'autre le produit de deux nombres premiers 23.83 et 13.73.

Le lecteur ajoutera d'autres exemples, s'il le désire, mais sans que jamais notre théorème puisse cesser d'avoir lieu. Pour nous, ce qui précède suffit.

# THÉORÈME

CONCERNANT

## LE PRODUIT D'UN NOMBRE PREMIER $8\mu+3$ PAR LE CARRÉ D'UN NOMBRE PREMIER $8\nu+7$.

(Extrait d'une Lettre de M. LIOUVILLE à M. BESGE.)

« ... Voici un théorème assez curieux au sujet du produit d'un » nombre premier donné $m$, de la forme $8\mu+3$, par le carré d'un » nombre premier $a$, donné aussi, mais de la forme $8\nu+7$. On pose » de toutes les manières possibles l'équation

$$a^2 m = x^2 + 2p^{4l+1} y^2,$$

» $p$ étant un nombre premier (naturellement de la forme $4\nu+1$) et » $x$, $y$ des entiers impairs, $x$ non divisible par $a$, et $y$ non divisible » par $p$. Le théorème dont je parle fournit une règle très-simple pour » décider à priori si le nombre N des décompositions de $a^2 m$ ainsi » obtenues est pair ou impair. En employant le signe connu introduit » par Legendre dans la théorie des résidus quadratiques, je trouve » que N est impair quand

$$\left(\frac{a}{m}\right) = 1,$$

» c'est-à-dire quand $a$ est résidu quadratique de $m$; au contraire N » est pair quand

$$\left(\frac{a}{m}\right) = -1,$$

» c'est-à-dire quand $a$ est non résidu quadratique de $m$.

» On a un exemple très-simple du premier cas en prenant $m=3$, » $a=7$. Comme

$$\left(\frac{7}{3}\right) = 1,$$

» on doit trouver alors N impair; et en effet $N = 3$, les équations ca-
» noniques étant

$$49.3 = 1^2 + 2.73.1^2,$$
$$49.3 = 5^2 + 2.61.1^2,$$
$$49.3 = 11^2 + 2.13.1^2.$$

» Vous aurez un exemple du second cas en prenant $m = 11$, $a = 7$.
» Comme

$$\left(\frac{7}{11}\right) = -1,$$

» notre théorème dit que N sera pair. Or on trouve en effet que
» $N = 6$. Voici les équations canoniques :

$$539 = 1^2 + 2.269.1^2,$$
$$539 = 5^2 + 2.257.1^2,$$
$$539 = 9^2 + 2.229.1^2,$$
$$539 = 15^2 + 2.157.1^3,$$
$$539 = 19^2 + 2.89.1^2,$$
$$539 = 23^2 + 2.5.1^2.$$

» Vous vous contenterez de ces deux exemples. Mais en terminant
» permettez-moi d'insister sur la condition de $x$ non divisible par $a$ :
» elle est essentielle. »

# THÉORÈMES

SUR

# LA DÉCOMPOSITION EN FACTEURS LINÉAIRES DES FONCTIONS HOMOGÈNES ENTIÈRES;

PAR M. L. PAINVIN.

1. Le *hessien* d'une fonction est le déterminant fonctionnel des dérivées premières de la fonction.

J'appellerai *hessiens dérivés du* $k^{\text{ième}}$ *ordre* d'une fonction les dérivées du $k^{\text{ième}}$ ordre prises par rapport aux éléments du hessien de cette fonction.

2. Les théorèmes que je vais démontrer sont résumés dans les énoncés suivants :

1° *Si le nombre des variables est au moins égal au degré de la fonction : pour qu'une fonction de degré p, à n variables, soit décomposable en un produit de p facteurs linéaires inégaux, il faut et il suffit que les hessiens dérivés du* $(n-p-1)^{\text{ième}}$ *ordre soient identiquement nuls, et, en outre, que tous les hessiens dérivés du* $(n-p)^{\text{ième}}$ *ordre soient dans un rapport identiquement constant avec la puissance* $(p-2)^{\text{ième}}$ *de la fonction.*

Ainsi, $u$ étant une fonction de degré $p$, H son hessien, $n$ le nombre des variables $(x_1, x_2, \ldots, x_n)$ qu'elle renferme, et $u_{rs}$ désignant la dérivée seconde $\frac{d^2 u}{dx_r\, dx_s}$, on devra avoir identiquement

$$1^\circ \quad \frac{d^{n-p-1}\mathrm{H}}{du_{r_1 s_1}\, du_{r_2 s_2} \ldots du_{r_{n-p-1} s_{n-p-1}}} = 0;$$

$$2^\circ \quad \frac{d^{n-p}\mathrm{H}}{du_{r_1 s_1}\, du_{r_2 s_2} \ldots du_{r_{n-p} s_{n-p}}} = (-1)^{p-1}(p-1)\lambda_{r_1 r_2 \cdots r_{n-p}}\lambda_{s_1 s_2 \cdots s_{n-p}}(u)^{p-2};$$

$r_1, r_2, \ldots, s_1, s_2, \ldots$ sont des nombres de la suite $1, 2, \ldots, n$, et les $\lambda_i$ représentent des constantes.

II° *Si le nombre des variables est au plus égal au degré de la fonction : pour qu'une fonction de degré p, à n variables, soit décomposable en p facteurs linéaires inégaux, il faut et il suffit que le hessien de la fonction soit identiquement divisible par la puissance* $(n-2)^{\text{ième}}$ *de la fonction.*

*Remarque I.* — Le cas particulier où le nombre des variables est égal au degré de la fonction est une conséquence de l'un ou de l'autre des deux énoncés précédents.

*Remarque II.* — L'application de ces théorèmes conduira à un nombre surabondant de relations ; il faudra se rappeler que le nombre des relations distinctes, pour qu'une fonction homogène de degré $p$, à $n$ variables, soit décomposable en facteurs linéaires inégaux, est donné par la formule

$$\frac{(p+1)(p+2)\ldots(p+n-1)}{1.2\ldots(n-1)} - p(n-1) - 1;$$

les relations excédantes seront une conséquence des autres.

3. Je commencerai par démontrer que les conditions énoncées ont lieu nécessairement lorsqu'on suppose la fonction décomposable en facteurs linéaires.

Premier cas. — Le nombre des variables est au moins égal au degré de la fonction.

Soit $u$ une fonction de degré $p$, $n$ le nombre des variables, et supposons cette fonction égale à un produit de $p$ facteurs linéaires de la forme

$$a_{r1}x_1 + a_{r2}a_2 + \ldots + a_{rn}x_n.$$

Soumettons cette fonction $u$ à la transformation linéaire

$$(1) \qquad y_r = a_{r1}x_1 + a_{r2}x_2 + \ldots + a_{rn}x_n;$$

dans ces dernières formules, $r$ désigne un quelconque des nombres de

la suite 1, 2,.., $n$; les valeurs $r = 1, 2, \ldots p$ reproduisent les $p$ facteurs de la fonction $u$. Cette substitution transformera la fonction $u$ en la fonction

(2) $$v = y_1 y_2 \cdots y_p.$$

Calculons le hessien et les hessiens dérivés de $u$ à l'aide des dérivées de la fonction $v$.

4. Posons

$$u_r = \frac{du}{dx_r}, \qquad u_{rs} = \frac{d^2 u}{dx_r dx_s},$$
$$v_r = \frac{dv}{dy_r}, \qquad v_{rs} = \frac{d^2 v}{dy_r dy_s},$$

et remarquons que

$$\left\{ \begin{array}{lll} v_{p+1} = 0, & v_{p+2} = 0, \ldots, & v_n = 0, \\ v_{r,p+1} = 0, & v_{r,p+2} = 0, \ldots, & v_{n,r} = 0. \end{array} \right.$$

Eu égard à ces relations, les formules (1) de transformation nous donneront

$$u_r = a_{1r} v_1 + a_{2r} v_2 + \ldots + a_{pr} v_p;$$

d'où l'on conclut

(3) $$\left\{ \begin{array}{l} u_{rs} = \dfrac{dv_1}{dx_s} a_{1r} + \dfrac{dv_2}{dx_s} a_{2r} + \ldots + \dfrac{dv_p}{dx_s} a_{pr}, \\ \dfrac{dv_r}{dx_s} = v_{r1} a_{1s} + v_{r2} a_{2s} + \ldots + v_{rp} a_{ps}. \end{array} \right.$$

Or si l'on se rappelle les principes sur lesquels repose la multiplication des déterminants, on voit que le hessien de $u$, ses hessiens dérivés du 1er, du 2e,..., du $(n-p-1)^{ième}$ ordre, sont des quantités identiquement nulles, puisque le nombre des produits qui entrent dans l'expression de $u_{rs}$ est inférieur au degré de ces déterminants. Ainsi nous voyons déjà que *tous les hessiens dérivés du* $(n-p-1)^{ième}$ *ordre de la fonction u sont identiquement nuls.*

5. Passons au calcul des hessiens dérivés du $(n-p)^{ieme}$ ordre.

Si l'on désigne par P le module de la substitution (1), et qu'on pose

$$(4)\qquad \lambda_{r_1 r_2 \cdots r_{n-p}} = \frac{d^{n-p}\mathrm{P}}{da_{r_1, p+1}\, da_{r_2, p+2} \cdots da_{r_{n-p}, n}}$$

(les seconds indices, dans le dénominateur, représentant des nombres fixes), les formules (3) nous donneront, pour les valeurs des hessiens dérivés du $(n-p)^{ième}$ ordre,

$$(5)\qquad \frac{d^{n-p}\mathrm{H}}{du_{r_1 s_1}\, du_{r_2 s_2} \cdots du_{r_{n-p} s_{n-p}}} = \lambda_{r_1 r_2 \cdots r_{n-p}} \cdot \lambda_{s_1 s_2 \cdots s_{n-p}} \begin{vmatrix} v_{11} & v_{12} & v_{13} \cdots & v_{1p} \\ v_{21} & v_{22} & v_{23} \cdots & v_{2p} \\ v_{31} & v_{32} & v_{33} \cdots & v_{3p} \\ \cdot & \cdot & \cdot & \cdot \\ v_{p1} & v_{p2} & v_{p3} \cdots & v_{pp} \end{vmatrix}$$

Or

$$v_{rr} = 0, \quad v_{rs} = \frac{v}{y_r y_s};$$

donc

$$\frac{d^{n-p}\mathrm{H}}{du_{r_1 s_1}\, du_{r_2 s_2} \cdots du_{r_{n-p} s_{n-p}}} = (-1)^{p-1}(p-1)\lambda_{r_1 r_2 \cdots r_{n-p}} \lambda_{s_1 s_2 \cdots s_{n-p}} \cdot v^{p-2}$$
$$= (-1)^{p-1}(p-1)\lambda_{r_1 r_2 \ldots} \lambda_{s_1 s_2 \ldots} \cdot u^{p-2};$$

ainsi les hessiens dérivés du $(n-p)^{ième}$ ordre sont identiquement proportionnels à la puissance $(p-2)^{ième}$ de la fonction.

6. Second cas. — Le nombre des variables est au plus égal au degré de la fonction.

Je remarque d'abord que le hessien étant un covariant de la fonction, toute relation entre le hessien et la fonction existera encore entre la fonction transformée par une substitution linéaire quelconque et le hessien de la fonction transformée. Choisissons, pour expressions des nouvelles variables, $n$ des facteurs dans lesquels se décompose la fonction. Cette fonction pourra donc s'écrire sous la forme

$$(6)\qquad u = y_1 y_2 \cdots y_n \mathrm{XYZ} \ldots \mathrm{U};$$

les variables sont $y_1, y_2, \ldots, y_n$; X, Y, etc., sont des fonctions linéaires de ces variables, et leur nombre est $p-n$.

Posons

$$(7)\qquad M_r = m_r y_r,\quad N_r = n_r y_r,\quad P_r = p_r y_r, \ldots,\quad Q_r = q_r y_r,$$

$$\text{où}\quad r = 1, 2, \ldots, n;$$

les X, Y, Z,..., U seront de la forme

$$(8)\qquad \begin{cases} X = M_1 + M_2 + \ldots + M_n, \\ Y = N_1 + N_2 + \ldots + N_n, \\ Z = P_1 + P_2 + \ldots + P_n, \\ \ldots\ldots\ldots\ldots\ldots \\ U = Q_1 + Q_2 + \ldots + Q_n. \end{cases}$$

Il s'agit de démontrer que le hessien de $u$ est divisible par $u^{n-2}$.

**7.** Posons encore, pour simplifier,

$$(9)\qquad \begin{cases} \mathfrak{P} = XYZ\ldots U, \\ a_r = \mathfrak{P}\left(\dfrac{M_r}{X} + \dfrac{N_r}{Y} + \dfrac{P_r}{Z} + \ldots + \dfrac{Q_r}{U}\right), \\ c_{rs} = \mathfrak{P}\left(\dfrac{M_r N_s + M_s N_r}{XY} + \dfrac{M_r P_s + M_s P_r}{XZ} + \ldots\right); \end{cases}$$

$$(10)\qquad \begin{cases} \alpha_{rr} = 2a_r + c_{rr}, \\ \alpha_{rs} = \mathfrak{P} + a_r + a_s + c_{rs}, \\ v = y_1 y_2 y_3 \ldots y_n, \end{cases}$$

on trouve que

$$(11)\qquad u_{rr} = \frac{v}{y_r^2}\alpha_{rr},\qquad u_{rs} = \frac{v}{y_r y_s}\alpha_{rs}.$$

Désignons par H le hessien de $u$; en combinant convenablement par voie d'addition les lignes et les colonnes de ce déterminant et en ayant

égard aux relations évidentes

$$(12)\quad \begin{cases} a_1 + a_2 + \ldots + a_n = (p-n)\mathfrak{P}, \\ c_{1r} + c_{2r} + \ldots + c_{nr} = c_{r1} + c_{r2} + \ldots + c_{rn} = (p-n-1)a_r, \end{cases}$$

on arrive rapidement à la valeur suivante de H

$$(13)\quad \mathrm{H} = \left(\frac{p-1}{p-n-1}\right)\mathfrak{P}^{n-2} \begin{vmatrix} -(p-2)\mathfrak{Q}+c_{11} & \mathfrak{Q}+c_{12}\cdots & \mathfrak{Q}+c_{1n} \\ \mathfrak{Q}+c_{21} & -(p-2)\mathfrak{Q}c_{22}\cdots & \mathfrak{Q}+c_{2n} \\ \mathfrak{Q}+c_{31} & \mathfrak{Q}+c_{32}\cdots & \mathfrak{Q}+c_{3n} \\ \cdots & \cdots & \cdots \\ \mathfrak{Q}+c_{n,1} & \mathfrak{Q}+c_{n,2}\cdots & -(p-2)\mathfrak{Q}+c_{n,n} \end{vmatrix}$$

où $\mathfrak{Q}$ représente la quantité $\frac{1}{p-1}\cdot\mathfrak{P}$.

*N. B.* — On devra traiter directement le cas où $p = n+1$.

8. Pour établir la proposition que nous avons en vue, il suffit de faire voir que ce déterminant est divisible par $\mathfrak{P}^{n-2}$ ou $\mathfrak{Q}^{n-2}$.

Dans ce but, on remarque d'abord que les $c_{rs}$ peuvent s'écrire sous la forme

$$(14)\quad c_{rs} = \frac{a_r a_s}{\mathfrak{P}} - \mathfrak{P} k_{rs},$$

en posant

$$(15)\quad k_{rs} = \frac{\mathrm{M}_r \mathrm{M}_s}{\mathrm{X}^2} + \frac{\mathrm{N}_r \mathrm{N}_s}{\mathrm{Y}^2} + \frac{\mathrm{P}_r \mathrm{P}_s}{\mathrm{Z}^2} + \ldots + \frac{\mathrm{Q}_r \mathrm{Q}_s}{\mathrm{U}^2}.$$

Si alors on développe par colonnes le déterminant qui est en facteur dans la valeur de H, on constate aisément que les déterminants partiels ainsi obtenus ont en facteur les quantités $\mathfrak{P}^{n-2}$.

L'espace que je dois occuper ne me permet pas de développer avec détails cette vérification qui n'offre pas d'ailleurs de sérieuses difficultés.

9. Les calculs que je viens d'exposer nous démontrent que, si une

fonction est décomposable en facteurs linéaires inégaux, les conditions énoncées au n° **2** sont nécessairement remplies.

Il reste maintenant à établir la *proposition réciproque*.

**10.** Supposons d'abord le nombre des variables supérieur au degré de la fonction. Soit une fonction $u$, de degré $p$, à $n$ variables; désignons par H son hessien, et admettons que

$$(16)\quad \left\{\begin{aligned} &\frac{d^{n-p-1}\mathrm{H}}{du_{r_1s_1}\,du_{r_2s_2}\ldots du_{r_{n-p-1}s_{n-p-1}}} = 0,\\ &\frac{d^{n-p}\mathrm{H}}{du_{r_1s_1}\ldots du_{r_2s_2}\ldots du_{r_{n-p}s_{n-p}}} = \lambda_{r_1r_2\ldots r_{n-p}}\lambda_{s_1s_2\ldots s_{n-p}}\cdot u^{p-2};\end{aligned}\right.$$

il s'agit de démontrer que la fonction $u$ est décomposable en facteurs linéaires. Représentons, pour un instant, par $h$ le déterminant $\dfrac{d^{n-p-1}\mathrm{H}}{du_{p+2,\,p+2}\,du_{p+3,\,p+3}\ldots du_{n,n}}$, nous aurons

$$u_{1r}\frac{dh}{du_{1r_1}} + u_{2r}\frac{dh}{du_{2r_1}} + \ldots + u_{p,r}\frac{dh}{du_{p,r_1}} + u_{p+1,r}\frac{dh}{du_{p+1,r_1}} = 0,$$

et cette relation aura lieu pour $r = r_1$, puisque $h$ est nul. En remplaçant les $\dfrac{dh}{du_{rs}}$ par leurs valeurs déduites de la seconde ligne des égalités (16), il vient

$$(17)\quad u_{1,r}\lambda_{1,p+2,\ldots,n} + u_{2r}\lambda_{2,p+2,\ldots,n} + \ldots + u_{p+1,r}\lambda_{p+1,p+2,\ldots,n} = 0,$$

et cette relation a lieu identiquement pour les valeurs 1, 2,..., $p+1$ de $r$. En raisonnant de la même manière sur $(n-p-1)$ déterminants de la forme $\dfrac{d^{n-p-1}\mathrm{H}}{du_{p+2,r_1}\,du_{p+3,r_2}\ldots du_{n,r_{n-p-1}}}$, on voit que l'identité (17) est encore vraie pour les valeurs $p+2$, $p+3$,..., $n$ de $r$. On conclut de cette identité

$$(18)\quad u_1\lambda_{1,p+2,\ldots,n} + u_2\lambda_{2,p+2,\ldots,n} + \ldots + u_{p+1}\lambda_{p+1,p+2,\ldots,n} = 0.$$

Par un raisonnement analogue, on obtiendra d'autres relations de la forme (18); on continuera cette déduction jusqu'à ce qu'on ait un nombre de relations égal à l'excès $(n-p)$ du nombre des variables sur le degré de la fonction. On aura ainsi le groupe des relations suivantes

$$(19)\quad \left\{\begin{array}{l} u_1\mu_{1,n} + u_2\mu_{2,n} + \ldots\ldots\ldots\ldots\ldots + u_{p+1}\mu_{p+1,n} = 0, \\ u_1\mu_{1,n-1} + u_2\mu_{2,n-1} + \ldots\ldots\ldots + u_p\ \mu_{p,n-1} \ + u_n\ \mu_{n,n-1} = 0, \\ u_1\mu_{1,n-2} + u_2\mu_{2,n-2} + \ldots + u_{p-1}\mu_{p-1,n-2} + u_{n-1}\mu_{n-1,n-2} + u_n\ \mu_{n,n-2} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right.$$

dont le nombre est $n-p$.

**11**. Ceci posé, effectuons la transformation linéaire

$$(20)\qquad x_r = \mu_{r,1}y_1 + \mu_{r,2}y_2 + \ldots + \mu_{r,n}y_n;$$

les $(n-p)$ dernières colonnes du module de cette substitution étant fournies par les relations (19); de sorte que la $n^{\text{ième}}$ colonne sera

$$\mu_{1,n},\ \mu_{2,n},\ \mu_{3,n},\ldots,\ \mu_{p+1,n},\ 0,\ 0,\ldots,\ 0,\ 0;$$

la $(n-1)^{\text{ième}}$ colonne sera

$$\mu_{1,n-1},\ \mu_{2,n-1},\ \mu_{3,n-1},\ldots,\ \mu_{p,n-1},\ 0,\ldots,\ 0,\ \mu_{n,n-1};$$

la $(n-2)^{\text{ième}}$ colonne sera

$$\mu_{1,n-2},\ \mu_{2,n-2},\ \mu_{3,n-3},\ldots,\ \mu_{p-1,n-2},\ 0,\ 0,\ldots,\ 0,\ \mu_{n-1,n-2},\ \mu_{n,n-2};$$

et ainsi de suite.

A l'aide des formules (20), la fonction $u$ se transformera en une fonction que je désignerai par $v$. On voit d'abord que la fonction transformée $v$ est indépendante des variables $y_{p+1}, y_{p+2},\ldots, y_n$; car, d'après les formules (20) et (19), on trouve

$$(21)\qquad \frac{dv}{dy_{p+1}} = 0,\quad \frac{dv}{dy_{p+2}} = 0,\ldots,\quad \frac{dv}{dy_n} = 0.$$

On conclut encore

$$(22)\qquad v_{r,p+1} = 0,\quad v_{r,p+2} = 0,\ldots,\quad v_{r,n} = 0.$$

Ainsi, si l'on a égard aux relations (16), on trouve que la fonction $u$ peut se transformer en une autre $v$, de même degré $p$, et ne renfermant plus que $p$ variables.

**12.** Je dis, en outre, que cette fonction $v$ est telle, que son hessien est dans un rapport identiquement constant avec la puissance $(p-2)^{ième}$ de la fonction.

Il suffit, pour le démontrer, de résoudre les formules (20) par rapport aux $y_r$ et de calculer les $u_{rs}$ en fonction de $v_{rs}$. En suivant alors une marche analogue à celle qui est indiquée dans le n° 4, et en s'appuyant sur les propriétés connues des déterminants réciproques, on constate que les identités (16) se réduisent toutes à la forme unique

$$\begin{vmatrix} v_{11} & v_{12}\cdots & v_{1p} \\ v_{21} & v_{22}\cdots & v_{2p} \\ \cdot & \cdot\;\cdot\;\cdot & \cdot \\ v_{p1} & v_{p2}\cdots & v_{pp} \end{vmatrix} = k.v^{p-2},$$

$k$ étant une constante; le hessien de la fonction $v$ est donc proportionnel à la puissance $(p-2)^{ième}$ de la fonction.

*Remarque.* — Ce même calcul nous montre que, dans les formules (20) de transformation, on ne devait pas étendre les relations (19) à plus de $(n-p)$ colonnes; car alors les hessiens dérivés du $(n-p)^{ième}$ ordre eussent été nuls, ce qui serait contraire aux hypothèses admises (16).

**13.** On voit par ce calcul que *la proposition réciproque* se trouve ramenée à l'examen du seul et unique cas où le nombre des variables est inférieur ou égal au degré de la fonction. Cette dernière question ne me semble pas, pour le moment, pouvoir être traitée par une analyse générale comme l'ont été toutes les questions qui précèdent. Cependant sa vérification est possible lorsque le degré de la fonction n'est pas trop élevé.

**14.** L'examen des cas où plusieurs des facteurs linéaires sont égaux, conduit à des théorèmes analogues. Je me contenterai d'énoncer la

proposition suivante dont la démonstration générale n'offre aucune difficulté.

*Pour qu'une fonction homogène, de degré p, à n variables, soit la puissance p^{ième} d'une fonction linéaire, il faut et il suffit que les hessiens dérivés du $(n-2)^{\text{ième}}$ ordre soient identiquement nuls.*

Ainsi, $u$ étant la fonction, on devra avoir identiquement

$$\begin{vmatrix} u_{rs} & u_{r_1 s} \\ u_{rs_1} & u_{r_1 s_1} \end{vmatrix} = 0$$

pour toutes les valeurs 1, 2, 3,..., $n$ des indices $r$, $r_1$, $s$, $s_1$.

# REMARQUES NOUVELLES

CONCERNANT

# LES NOMBRES PREMIERS DE LA FORME $24\mu + 7$;

PAR M. J. LIOUVILLE.

Déjà nous nous sommes occupés des nombres premiers de la forme $24\mu + 7$. On a vu en particulier (dans le cahier de novembre 1859) que si $p$ désigne un tel nombre, on peut toujours poser (un nombre impair de fois) l'équation

$$2p = x^2 + q^{4l+1} y^2,$$

$x$ et $y$ étant des entiers impairs et $q$ un nombre premier de la forme $24\nu + 13$, qui ne divise pas $y$.

Avec la forme imposée à $q$, il est évident que $x$ doit être premier à 3, et réciproquement dès que $x$ est premier à 3, $q$ ne peut avoir que la forme indiquée. Quant à $y$, on s'assurera sans peine qu'il n'est jamais divisible par 3. Mais en prenant $x$ multiple de 3 et $q$ de la forme $24\nu + 5$, on pourrait aussi représenter $2p$. De là un théorème nouveau qui complétera, pour ainsi dire, celui que nous venons de rappeler. Les nombres premiers de la forme $24\mu + 7$ donnent en outre lieu à plusieurs remarques intéressantes qu'on trouvera ci-après. J'entre en matière.

*Théorème I.* — « Pour tout nombre premier $p$, de la forme » $24\mu + 7$, on peut poser un nombre impair de fois l'équation

$$2p = 9x^2 + q^{4l+1} y^2,$$

» $x$ et $y$ étant des entiers impairs, et $q$ un nombre premier qui ne divise pas $y$. »

Cet énoncé n'impose aucune condition au nombre premier $q$; mais

comme, d'après la forme $24\mu + 7$ assignée à $p$, on a

$$2p \equiv 6 \pmod{8}, \qquad 2p \equiv 2 \pmod{3},$$

il s'ensuit qu'on aura nécessairement

$$q \equiv 5 \pmod{8}, \qquad q \equiv 2 \pmod{3}.$$

Donc $q$ sera toujours de la forme $24\nu + 5$, indiquée tout à l'heure.

Vérifions notre théorème sur quelques exemples. Et d'abord soit $p = 7$ ; nous aurons, comme il le faut, l'équation canonique

$$2.7 = 9.1^2 + 5.1^2.$$

Pour $p = 31$, on a de même

$$2.31 = 9.1^2 + 53.1^2.$$

Je trouve aussi une équation canonique pour $p = 79$, savoir

$$2.79 = 9.1^2 + 149.1^2.$$

Enfin on en a une pour $p = 103$. C'est

$$2.103 = 9.1^2 + 197.1^2.$$

L'équation

$$2.103 = 9.3^2 + 5^3.1^2$$

a dû être rejetée, bien que 5 soit un nombre premier, parce que l'exposant 3 n'est pas de la forme $4l + 1$.

*Remarque.* — Si, désignant toujours par $p$ un nombre premier donné de la forme $24\mu + 7$, on posait

$$2p = x^2 + q^{4l+1}y^2,$$

en prenant pour $x$ et $y$ des entiers impairs *quelconques* et en assujettissant le nombre premier $q$ à la seule condition de ne pas diviser $y$, le nombre N des décompositions de $2p$ ainsi obtenues serait toujours

pair, mais au moins égal à 2, comme étant la somme de deux nombres impairs $N_1$, $N_2$ respectivement relatifs aux deux hypothèses de $x$ premier à 3 (ou de $q = 24\nu + 13$) et de $x$ multiple de 3 (ou de $q = 24\nu + 5$). Cela résulte du nouveau théorème que nous venons de donner, combiné avec celui que nous avions donné en 1859.

*Théorème II.* — « Pour tout nombre premier $p$, de la forme » $24\mu + 7$, on peut poser un nombre impair de fois l'équation

$$2p = 3x^2 + q^{4l+1} y^2,$$

» $x$ et $y$ étant des entiers impairs, et $q$ un nombre premier non di» viseur de $y$. »

Notre énoncé n'impose aucune condition au nombre premier $q$; mais il est évident qu'il ne pourra manquer de vérifier les deux congruences

$$q \equiv 3 \pmod{8}, \qquad q \equiv 2 \pmod{3}.$$

Il sera donc nécessairement de la forme $24\nu + 11$.

Passons aux vérifications numériques. D'abord pour

$$p = 7,$$

on a l'équation canonique

$$2.7 = 3.1^2 + 11.1^2.$$

On en a une également pour

$$p = 31,$$

savoir

$$2.31 = 3.1^2 + 59.1^2.$$

Soit à présent

$$p = 79.$$

Les équations canoniques seront alors au nombre de trois :

$$2.79 = 3.3^2 + 131.1^2,$$
$$2.79 = 3.5^2 + 83.1^2,$$
$$2.79 = 3.7^2 + 11.1^2.$$

J'en trouve aussi trois pour

$$p = 103.$$

Les voici :

$$2.103 = 3.3^2 + 179.1^2,$$

$$2.103 = 3.5^2 + 131.1^2,$$

$$2.103 = 3.7^2 + 59.1^2.$$

Toujours notre théorème a lieu, mais voilà assez d'exemples.

*Théorème III.* — « Pour tout nombre premier $p$, de la forme » $24\mu + 7$, on peut poser un nombre impair de fois l'équation

$$p = 2x^2 + q^{4l+1}y^2,$$

» $x$ et $y$ étant des entiers impairs, non divisibles par 3, et $q$ un nombre » premier non diviseur de $y$. »

Puisque $x$ est supposé premier à 3, on aura

$$2x^2 \equiv 2 \pmod{3}.$$

Mais déjà on a

$$p \equiv 1 \pmod{3}.$$

L'équation

$$p = 2x^2 + q^{4l+1}y^2$$

entraîne donc la congruence

$$q^{4l+1}y^2 \equiv -1 \pmod{3}.$$

La condition relative à $y$ de ne pas être divisible par 3 sera donc remplie d'elle-même ; mais de plus on voit que nécessairement

$$q \equiv -1 \pmod{3}.$$

Il est d'ailleurs aisé de voir que l'équation

$$p = 2x^2 + q^{4l+1}y^2,$$

où l'on a

$$p \equiv 7 \pmod{8},$$

entraîne cette seconde congruence

$$q \equiv 5 \pmod{8}.$$

Il suit de là que $q$ ne peut être que de la forme $24\nu + 5$.

Soit d'abord

$$p = 7,$$

et nous aurons l'équation canonique

$$7 = 2.1^2 + 5.1^2.$$

On en a une également pour

$$p = 31,$$

savoir

$$31 = 2.1^2 + 29.1^2;$$

une aussi pour

$$p = 79,$$

car

$$79 = 2.5^2 + 29.1^2.$$

Notre théorème se vérifie aussi pour

$$p = 103;$$

mais alors il y a trois équations canoniques

$$103 = 2.1^2 + 101.1^2,$$
$$103 = 2.5^2 + 53.1^2,$$
$$103 = 2.7^2 + 5.1^2.$$

Nous ne pousserons pas plus loin les exemples.

Dans la forme

$$2x^2 + q^{4l+1}y$$

que nous venons d'employer pour représenter le nombre premier donné $p$, de la forme $24\mu + 7$, nous avons supposé $x$ premier à 3. Prenons à présent $x$ multiple de 3, ou plutôt remplaçons $x$ par $3x$, et nous aurons la proposition nouvelle que voici :

*Théorème IV.* — « On désigne par $p$ un nombre premier donné,

» de la forme $24\mu + 7$, et on pose de toutes les manieres possibles l'é-
» quation

$$p = 18x^2 + q^{4l+1}y^2,$$

» $x$ et $y$ étant des entiers impairs, et $q$ un nombre premier (naturelle-
» ment de la forme $24\nu + 13$) qui ne divise pas $y$. Le nombre N des
» décompositions de $p$ ainsi obtenues est tantôt pair et tantôt impair;
» mais on a toujours $N \equiv \mu$ (mod. 2). »

En d'autres termes N est pair quand $\mu$ est pair, mais impair quand $\mu$ est impair; ou ce qui revient au même, N est pair quand $p = 48k + 7$, mais impair quand $p = 48k + 31$.

Il suit de notre théorème que l'on doit trouver N pair pour

$$p = 7$$

et pour

$$p = 103,$$

mais impair pour

$$p = 31$$

et pour

$$p = 79.$$

Or je trouve en effet

$$N = 0$$

pour les deux premiers nombres 7 et 103, tandis que pour les deux autres, 31 et 17, on a

$$N = 1,$$

en vertu des équations canoniques

$$31 = 18.1^2 + 13.1^2$$

et

$$79 = 18 + 61.1^2.$$

Notre théorème est donc vérifié sur ces exemples, et il le sera également sur tous ceux qu'on pourra vouloir ajouter.

SUR LES

# DEUX FORMES QUADRATIQUES

## $x^2 + y^2 + z^2 + 2t^2$, $x^2 + 2(y^2 + z^2 + t^2)$;

**Par M. J. LIOUVILLE.**

1. Soit $n$ un nombre entier donné quelconque. Désignons par $A(n)$ le nombre des représentations de $n$ par la forme

$$x^2 + y^2 + z^2 + 2t^2,$$

c'est-à-dire le nombre des solutions de l'équation indéterminée

$$n = x^2 + y^2 + z^2 + 2t^2,$$

où les entiers $x$, $y$, $z$, $t$ peuvent être indifféremment positifs, nuls ou négatifs, deux solutions étant regardées comme différentes quand $x$, $y$, $z$, $t$ n'y ont pas identiquement les mêmes valeurs. Désignons de même par $B(n)$ le nombre des représentations de $n$ par la forme

$$x^2 + 2(y^2 + z^2 + t^2),$$

c'est-à-dire le nombre des solutions de l'équation

$$n = x^2 + 2(y^2 + z^2 + t^2).$$

Il s'agit de donner des règles simples pour trouver à priori $A(n)$ et $B(n)$. On s'occupe à la fois des deux formes

$$x^2 + y^2 + z^2 + 2t^2$$

et

$$x^2 + 2(y^2 + z^2 + t^2),$$

parce qu'elles ont entre elles une liaison intime.

2. Comme $n$ peut être pair ou impair, nous poserons généralement

$$n = 2^{\alpha} m,$$

$m$ étant un entier impair et l'exposant $\alpha$ pouvant se réduire à zéro. Il faudra avoir égard aux diverses valeurs de $\alpha$, et aussi à la forme linéaire de $m$ (mod. 8), en distinguant deux cas suivant que l'on a

$$m = 8k \pm 1$$

ou

$$m = 8k \pm 3.$$

Le calcul de $\mathrm{A}(n)$ et de $\mathrm{B}(n)$ exigera en outre celui d'une certaine fonction numérique de $m$, que nous allons définir.

Soit $d$ un quelconque des diviseurs de $m$ (dont 1 et $m$ font toujours partie), et désignons par $\delta$ le diviseur conjugué à $d$, en sorte que

$$m = d\delta.$$

La fonction numérique dont nous voulons parler s'exprimera par

$$\sum (-1)^{\frac{\delta^2 - 1}{8}} d,$$

le signe sommatoire portant sur tous les groupes $d$, $\delta$. On pourrait encore l'écrire

$$\sum \left(\frac{2}{\delta}\right) d,$$

en employant le signe

$$\left(\frac{a}{b}\right)$$

de Legendre avec la signification plus étendue que lui a donnée Jacobi.

Pour abréger nous désignerons, dans tout ce qui va suivre, la somme

$$\sum (-1)^{\frac{\delta^2 - 1}{8}} d$$

par la simple lettre S. On voit que quand

$$m = 8k \pm 1,$$

S est l'excès de la somme des diviseurs de $m$ qui sont de la forme $8k \pm 1$ sur celle des diviseurs de $m$ qui sont de la forme $8k \pm 3$. Au contraire, quand

$$m = 8k \pm 3,$$

S est l'excès de la somme des diviseurs de $m$ de la forme $8k \pm 3$ sur celle des diviseurs de $m$ de la forme $8k \pm 1$. Pour $m = 1, 3, 5, 7, 9$, etc., on a successivement $S = 1, 2, 4, 8, 7$, etc.

5. Ceci expliqué, je dirai d'abord que l'on a, suivant la nature du nombre impair $m$,

$$A(m) = 6S, \quad B(m) = 2S,$$

quand

$$m = 8k \pm 1;$$

mais

$$A(m) = 10S, \quad B(m) = 6S,$$

quand

$$m = 8k \pm 3.$$

De ces quatre équations deux seulement ont dû être tirées de mes *formules générales;* car on prouve aisément à priori que

$$A(8k \pm 1) = 3B(8k \pm 1)$$

et

$$3A(8k \pm 3) = 5B(8k \pm 3).$$

Des raisonnements arithmétiques très-simples donnent aussi les valeurs de $A(2m)$, $A(4m)$, etc., en partant des valeurs de $A(m)$, $B(m)$. On arrive de cette manière aux formules ci-après :

$$A(2^\alpha m) = 2(2^{\alpha+2} - 1)S$$

pour $m = 8k \pm 1$, et

$$A(2^\alpha m) = 2(2^{\alpha+2} + 1)S$$

pour $m = 8k \pm 3$. Ces formules subsistent même pour $\alpha = 0$, et on les réunirait en une seule en écrivant

$$A(2^\alpha m) = 2\left[2^{\alpha+2} - (-1)^{\frac{m^2-1}{8}}\right]S.$$

La valeur de $A(n)$ est donc connue quel que soit $n$; et celle de $B(n)$ pour $n$ pair s'en conclut, car on a

$$B(2^\alpha n) = A(2^{\alpha-1} n),$$

à partir de $\alpha = 1$.

4. Appliquons nos formules aux cas les plus simples. Elles nous donnent d'abord

$$A(1) = 6, \quad B(1) = 2;$$

or ce résultat est confirmé par les équations canoniques

$$1 = (\pm 1)^2 + 0^2 + 0^2 + 2.0^2$$

et

$$1 = (\pm 1)^2 + 2(0^2 + 0^2 + 0^2),$$

dans la première desquelles $(\pm 1)^2$ peut être reporté à la seconde et à la troisième place.

Je trouve ensuite

$$A(3) = 20, \quad B(3) = 12,$$

ce qui est confirmé par les équations

$$3 = (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 + 2.0^2,$$

$$3 = (\pm 1)^2 + 0^2 + 0^2 + 2.(\pm 1)^2,$$

et

$$3 = (\pm 1)^2 + 2[(\pm 1)^2 + 0^2 + 0^2),$$

en y faisant les permutations convenables.

Soit en dernier lieu, $n = 2$. Il vient

$$A(2) = 14, \quad B(2) = 6,$$

ce qui résulte en effet des équations

$$2 = (\pm 1)^2 + (\pm 1)^2 + 0^2 + 2.0^2,$$

$$2 = 0^2 + 0^2 + 0^2 + 2(\pm 1)^2,$$

et

$$2 = 0^2 + 2\left[(\pm 1)^2 + 0^2 + 0^2\right].$$

5. En m'occupant des équations

$$n = x^2 + y^2 + z^2 + 2t^2$$

et

$$n = x^2 + 2(y^2 + z^2 + t^2),$$

j'ai considéré à la fois les solutions propres (où $x$, $y$, $z$, $t$ n'ont pour facteur commun que l'unité) et les solutions impropres (où $x$, $y$, $z$, $t$ sont divisibles par un même nombre $> 1$). On pourrait demander seulement le nombre des solutions propres; mais je ne m'arrêterai pas à cette question nouvelle qui n'offre aucune difficulté.

6. En terminant j'indiquerai celles de nos *formules générales* dont nous nous sommes servis pour obtenir les résultats qui précèdent. C'est d'abord la formule (F) de notre troisième article (cahier de juin 1858, p. 208) : il faut y faire

$$f(x) = \cos\left(\frac{x\pi}{4}\right).$$

C'est ensuite la formule (I) de notre cinquième article (cahier d'août, page 277) où l'on prendra pour $f(x)$ la même valeur. On devra se rappeler les propriétés de la fonction $\rho(m)$ qui marque l'excès du nombre des diviseurs de $m$ de la forme $4g + 1$ sur celui des diviseurs de la forme $4g + 3$ : on sait quel rôle joue la fonction $\rho(m)$ relativement à la décomposition des nombres en deux carrés, c'est-à-dire relativement à la forme quadratique $x^2 + y^2$. Mais il faudra de plus considérer la fonction $\xi(m)$ qui joue un rôle analogue pour la forme $x^2 + 2y^2$, et qui exprime l'excès du nombre des diviseurs de $m$ de l'une des deux formes $8k + 1$, $8k + 3$ sur celui des diviseurs $8k + 5$,

$8k+7$. En faisant comme plus haut $m = d\delta$, on a

$$\xi(m) = \sum (-1)^{\frac{\delta-1}{2}+\frac{\delta^2-1}{8}}.$$

En général on doit attacher un grand prix aux fonctions numériques suivantes qui sont décomposables en facteurs et qui se présentent sans cesse dans nos recherches :

$$\zeta_\mu(m) = \sum d^\mu, \qquad \xi_\mu(m) = \sum (-1)^{\frac{\delta-1}{2}+\frac{\delta^2-1}{8}} d^\mu,$$

$$\rho_\mu(m) = \sum (-1)^{\frac{\delta-1}{2}} d^\mu, \quad \omega_\mu(m) = \sum (-1)^{\frac{\delta^2-1}{8}} d^\mu.$$

Je continue à supposer $m$ impair. On voit que la quantité désignée ci-dessus par S est précisément $\omega_1(m)$. Au reste nos quatre fonctions sont comprises dans celle-ci :

$$\sum \left(\frac{a}{\delta}\right) d^\mu,$$

où $a$ est un entier donné, et que nous aurons aussi à employer dans toute sa généralité.

# THÉORÈMES

SUR

# LE CÔNE DE RÉVOLUTION;

PAR M. WOEPCKE.

Si par deux points quelconques de l'axe d'un même cône, on mène deux plans tels, que le carré du sinus de l'angle générateur du cône soit la moyenne arithmétique entre les carrés des sinus des inclinaisons de l'axe du cône sur les deux plans coupants, on obtient une ellipse et une hyperbole dans lesquelles le rapport des axes est le même.

Si l'on mène dans un même cône, et par le même point de son axe, deux points tels, que le carré de la valeur inverse du sinus de l'angle générateur du cône soit la moyenne arithmétique entre les carrés des valeurs inverses des sinus des inclinaisons de l'axe du cône sur les deux plans coupants, on obtient une ellipse et une hyperbole dont les grands axes et les paramètres sont inversement proportionnels.

En désignant par $\alpha$ l'angle générateur du cône, par $\beta$ l'inclinaison de son axe sur le plan coupant, les sections produites dans des cônes quelconques par des plans coupants quelconques sont semblables, si le rapport $\frac{\cos\alpha}{\cos\beta}$ reste le même.

Dans toutes les sections qui rendent $\tang\alpha = \sin\beta$, le segment compris sur l'axe du cône entre le sommet et le plan coupant est la moitié du petit axe de la section.

Dans toutes les sections qui rendent $\cot\alpha = \sin\beta$, le segment compris sur l'axe du cône entre le sommet et le plan coupant est égal au demi-paramètre de la section.

Dans toutes les sections produites par des plans perpendiculaires à

une arête du cône, la partie du grand axe de la section comprise entre cette arête et l'axe du cône est égale au demi-paramètre.

Si l'on coupe une série de cônes décrits autour d'un même axe avec des angles générateurs quelconques par un cylindre de révolution décrit autour du même axe, et si l'on mène une série de plans parallèles par les centres des cercles en lesquels les cônes sont rencontrés par le cylindre, les sections produites par chacun des plans parallèles dans le cône correspondant auront toutes le même paramètre.

Si l'on coupe, à la même distance du sommet, l'axe d'un cône dont l'angle générateur est $\alpha$, par un plan formant avec l'axe un angle $\beta$, et l'axe d'un cône dont l'angle générateur est $\beta$, par un plan formant avec l'axe l'angle $\alpha$, on obtient une ellipse et une hyperbole dont les grands axes et les paramètres sont inversement proportionnels. Les paramètres sont changés dans le rapport de $\frac{\cos\alpha}{\cos\beta}$ et les grands axes dans le rapport de $\frac{\cos\beta}{\cos\alpha}$. En même temps les deux sphères inscrites au cône qui touchent le plan coupant aux foyers de la section changent de place, mais non de grandeur.

SUR

# UN CERTAIN GENRE DE DÉCOMPOSITIONS D'UN ENTIER EN SOMMES DE CARRÉS;

Par M. J. LIOUVILLE.

Les décompositions d'un entier $n$ en sommes de carrés dont je veux m'occuper ici offrent ce caractère particulier que, lorsqu'il y a dans l'expression de $n$ des carrés impairs, on en prend la racine positivement et on les range avant les autres, dans un ordre du reste quelconque. Le double signe est conservé pour les racines des carrés pairs, à moins qu'elles ne se réduisent à zéro.

J'introduis à ce sujet une notation nouvelle. Je désigne par

$$\mathrm{N}(n, p, q)$$

le nombre des décompositions de $n$ en $p$ carrés dont les $q$ premiers sont impairs et à racines positives, tandis que les $(p-q)$ derniers sont pairs et à racines indifféremment positives, nulles ou négatives. En d'autres termes, nous désignons par $\mathrm{N}(n, p, q)$ le nombre des solutions de l'équation

$$n = i_1^2 + i_2^2 + \ldots + i_q^2 + \varpi_1^2 + \varpi_2^2 + \ldots + \varpi_{p-q}^2,$$

dont le premier membre est donné, et où la lettre $i$ désigne des entiers positifs impairs, tandis que les entiers $\varpi$ sont indifféremment positifs, nuls ou négatifs. On prendra $q = 0$ si tous les carrés sont pairs.

Soit par exemple $n = 2m$, $m$ étant impair, et $p = 12$, en sorte qu'il s'agisse des décompositions du double d'un entier impair en une somme de douze carrés. Les décompositions spéciales que nous considérons ne pourront être que de trois espèces; car des douze carrés dont la somme exprime $2m$, deux, six ou dix seront impairs et les

autres pairs. Les valeurs à donner à $q$ seront donc 2, 6, 10. D'après notre notation $N(2m, 12, 2)$, $N(2m, 12, 6)$, $N(2m, 12, 10)$ répondent respectivement à ces trois cas. Les autres valeurs de $N(2m, 12, q)$ sont nulles. Il est évident que pour $m = 1$, on a

$$N(2, 12, 2) = 1, \quad N(2, 12, 6) = 0, \quad N(2, 12, 6) = 0.$$

Pour $m = 3$, on trouve facilement

$$N(6, 12, 2) = 20, \quad N(2, 12, 6) = 1, \quad N(2, 12, 10) = 0,$$

la valeur de $N(6, 12, 2)$ dépendant de l'équation

$$6 = 1^2 + 1^2 + (\pm 2)^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2,$$

où $(\pm 2)^2$ peut prendre dix places distinctes. On trouve de même pour $m = 5$,

$$N(10, 12, 2) = 182, \quad N(10, 12, 6) = 12, \quad N(10, 12, 10) = 1.$$

Et ainsi de suite.

Le nombre complet des *représentations* de l'entier $n$ par une somme de $p$ carrés, c'est-à-dire le nombre des solutions de l'équation

$$n = x_1^2 + x_2^2 + \ldots + x_p^2,$$

où $x_1, x_2, \ldots, x_p$ sont des entiers indifféremment pairs ou impairs, positifs, nuls ou négatifs, sera désigné convenablement par

$$N(n, p).$$

On le déduirait immédiatement des nombres partiels $N(n, p, 0)$, $N(n, p, 1)$, etc., si ceux-ci étaient connus; car on passe de nos décompositions aux représentations en donnant aux entiers impairs marqués par la lettre $i$ le double signe $\pm$, puis permutant les $i$ et les $\varpi$ et faisant la somme des résultats.

Ainsi dans l'exemple ci-dessus de $p = 12$, $n = 2m$, $m$ impair, la

valeur de $N(2m, 12)$ est égale à

$$\frac{11.12}{1.2}[2^2 N(2m, 12, 2) + 2^{10} N(2m, 12, 10)] + 2^6 \cdot \frac{7.8.9.10.11.12}{1.2.3.4.5.6} N(2m, 12, 6),$$

et peut s'écrire

$$N(2m, 12) = 264[N(2m, 12, 2) + 224 N(2m, 12, 6) + 256 N(2m, 12, 10)].$$

Nous verrons bientôt qu'on peut tirer parti de ce résultat.

Les décompositions indiquées par la notation

$$N(n, p, q)$$

donnent lieu à une théorie étendue et fort intéressante. Mais je ne veux communiquer ici que deux théorèmes relatifs au cas de $n = 2m$, $m$ impair, et où figureront les fonctions numériques que je désigne par $\zeta_\mu(m)$, $\rho_\mu(m)$, dont je rappelle la définition. Soit $d$ un diviseur de $m$, $\delta$ le diviseur conjugué, de façon que $m = d\delta$ : on a

$$\zeta_\mu(m) = \sum d^\mu,$$

et

$$\rho_\mu(m) = \sum (-1)^{\frac{\delta-1}{2}} d^\mu.$$

Quand $\mu = 0$, au lieu de $\zeta_0(n)$ et $\rho_0(n)$, j'écris simplement $\zeta(m)$ et $\rho(m)$.

*Théorème I.* « Si $m$ désigne un entier impair à volonté et $\nu$ un » entier donné, on pourra poser, pour toutes les valeurs de $m$,

$$\zeta_{2\nu-1}(m) = N(2m, 4\nu, 2) + A_1 N(2m, 4\nu, 6) + \ldots + A_{\nu-1} N(2m, 4\nu, 4\nu-2),$$

» $A_1, A_2, \ldots, A_{\nu-1}$ étant des constantes, c'est-à-dire ayant des valeurs » indépendantes de $m$, mais qui changent quand $\nu$ change. »

Notre équation peut s'écrire

$$\zeta_{2\nu-1}(m) = \sum A_s N(2m, 4\nu, 4s+2),$$

la sommation portant sur $s$ dont les valeurs successives sont 0, 1, 2,..., $\nu - 1$.

On a

$$A_0 = 1, \quad A_{\nu-1} = 16^{\nu-1},$$

et en général

$$A_{\nu-s-1} = 16^{\nu-2s-1} A_s.$$

Les coefficients $A_s$ se déterminent d'ailleurs aisément au moyen des plus petites valeurs de $m$.

En passant aux cas particuliers, on trouve, pour $\nu = 1$,

$$\zeta_1(m) = N(2m, 4, 2),$$

puis, pour $\nu = 2$,

$$\zeta_3(m) = N(2m, 8, 2) + 16 N(2m, 8, 6),$$

puis, pour $\nu = 3$,

$$\zeta_5(m) = N(2m, 12, 2) + 224 N(2m, 12, 6) + 256 N(2m, 12, 10).$$

Et ainsi de suite.

Laissant de côté les deux premières équations qui répondent à des théorèmes démontrés par Jacobi, j'observe que la troisième fournit $N(2m, 12)$; car, d'après la valeur de $N(2m, 12)$ indiquée plus haut et comparée à celle de $\zeta_5(m)$, il vient

$$N(2m, 12) = 264 \zeta_5(m),$$

ce qui s'accorde avec le théorème que j'ai donné dans le cahier de mai 1860 et qu'on peut établir aussi par d'autres procédés.

J'observerai en passant que la valeur de $N(m, 12)$ semble moins simple. Elle dépend non-seulement de $\zeta_5(m)$ et $\zeta_1(m)$, mais encore de la somme

$$\sum s^4$$

des carrés des premiers termes dans l'ensemble des représentations de $m$ par une somme de quatre carrés $s^2 + s'^2 + s''^2 + s'''^2$. Je trouve

$$N(m, 12) = 8\zeta_5(m) - 16m^2\zeta_1(m) + 16\sum s^4.$$

Si $m$ était pair, on aurait aisément $\sum s^4$, mais pour $m$ impair la difficulté paraît grande. On pourrait encore faire dépendre $N(m, 12)$ de $N(4m, 12, 12)$, en vertu de l'équation

$$N(m, 12) = 24\zeta_5(m) - 2^{12}N(4m, 12, 12).$$

Mais ce n'est pas le lieu d'approfondir ces questions délicates.

*Théorème II.* « Si $m$ désigne un entier impair à volonté et $\nu$ un en-
» tier donné, on pourra trouver des constantes

$$B_0, B_1, \ldots, B_\nu$$

» telles, qu'on ait, pour toutes les valeurs de $m$,

$$\rho_{2\nu}(m) = \sum B_s N(2m, 4\nu + 2, 4s + 2),$$

» le signe sommatoire portant sur $s$ dont les valeurs sont $0, 1, 2, \ldots, \nu - 1, \nu$. »

Les coefficients $B_s$ sont constants en ce sens qu'ils ne dépendent pas de $m$. Ils changent avec $\nu$; mais on a toujours $B_0 = 1$, et dès que $\nu$ est $> 0$, on a $B_\nu = 0$. Au surplus les coefficients $B_s$ se calculent pour chaque valeur de $\nu$ au moyen des plus petites valeurs de $m$.

Pour $\nu = 0$, notre équation donne

$$\rho(m) = N(2m, 2, 2),$$

ce qui répond au théorème si connu sur la décomposition de $2m$ en deux carrés impairs. Pour $\nu = 1$, elle donne

$$\rho_2(m) = N(2m, 6, 2);$$

puis, pour $\nu = 2$,

$$\rho_4(m) = N(2m, 10, 2) + 64N(2m, 10, 6);$$

et ainsi de suite.

Je me contenterai de faire observer que la dernière des équations que je viens d'écrire conduit assez facilement à la valeur de $N(2m, 10)$ quand $m$ est de la forme $4g+3$, auquel cas on peut prouver que

$$N(2m, 10, 2) = 16 N(2m, 10, 6), \quad N(2m, 10, 10) = 0.$$

ce qui permet d'exprimer $N(2m, 10, 2)$ et $N(2m, 10, 6)$ au moyen de $\rho_4(m)$, et puisque les autres valeurs de $N(2m, 10, q)$ sont nulles, d'en conclure $N(2m, 10)$. J'ai trouvé ainsi :

$$N(2m, 10) = 12.17.\rho_4(m).$$

Dans la même supposition sur $m$, Eisenstein a obtenu

$$N(m, 10) = 12\rho_4(m).$$

Il faut donc que, pour $m = 4g+3$, on ait généralement

$$N(2m, 10) = 17 N(m, 10);$$

et c'est en effet ce qu'on peut démontrer à priori par un raisonnement arithmétique très-simple.

Il y aurait, nous le répétons, bien des choses à dire au sujet des fonctions $N(n, p, q)$ et d'autres fonctions analogues. Mais tout cela viendra à son temps.

# EXTRAIT D'UNE LETTRE DE M. BESGE A M. LIOUVILLE.

« Soient A et $a$ deux entiers impairs, $a$ premier absolu, A premier à $a$ et diviseur de $t^2 + a$. On sait qu'on pourra poser

$$A^{\mu} = x^2 + ay^2,$$

$x$ et $y$ étant des entiers premiers entre eux. Les valeurs de $\mu$ convenables sont en nombre infini ; mais je ne considère ici que la plus petite. Il arrivera souvent qu'elle soit paire, et elle le sera sans aucun doute si A est non résidu quadratique de $a$, ou encore si $a$ est de la forme $4n + 1$ et A de la forme $4n + 3$. Or lorsque l'on a $\mu = 2\nu$, je dis que $y$ est impair. En effet si l'on avait $y = 2^{\alpha} z$, l'équation

$$(A^{\nu} - x)(A^{\nu} + x) = 2^{2\alpha} az^2,$$

où je prends $x$ indifféremment positif ou négatif, se décomposerait de l'une des deux manières suivantes :

$$A^{\nu} - x = 2p^2, \qquad A^{\nu} + x = 2^{2\alpha - 1} aq^2,$$

ou

$$A^{\nu} - x = 2ap^2, \qquad A^{\nu} + x = 2^{2\alpha - 1} q^2,$$

de sorte qu'en ajoutant et divisant par 2, on trouverait

$$A^{\nu} = m^2 + an^2,$$

$\nu$ étant plus petit que $\mu$, qu'on a supposé minimum.

» Puisque $y$ est impair, $x$ doit être pair, et dès lors les deux facteurs au premier membre de l'équation

$$(A^{\nu} - x)(A^{\nu} + x) = ay^2$$

sont impairs. Cette équation se décomposera donc en deux telles que celles-ci :

$$A^\nu - x = p^2, \qquad A^\nu + x = aq^2,$$

$p^2$ et $aq^2$ étant premiers entre eux. Dans les conditions où nous nous sommes placés, il vient donc

$$2A^\nu = p^2 + aq^2,$$

et il est aisé de voir que $\nu$ est à son tour un minimum, car s'il existait un exposant moindre, convenable à une telle équation, en élevant au carre et divisant par 4, on retrouverait pour une puissance de A, avec un exposant double de celui-là, partant $< \mu$, la forme $x^2 + ay^2$.

L'exposant $\nu$ peut être pair ou impair; mais le premier cas reste seul possible quand 2A est non résidu quadratique de $a$, et le second quand 2 est non résidu. Ni l'un, ni l'autre ne pouvant avoir lieu quand 2 et 2A à la fois sont non résidus quadratiques de $a$, on voit qu'alors l'équation $\mu = 2\nu$ doit être impossible, en sorte que $\mu$ ne peut être qu'impair. Il en est évidemment de même quand $a$ est de la forme $4n + 3$, ou quand, $a$ étant de la forme $8n + 5$, A est de la forme $4n + 1$. J'ajoute que quand $a$ est de la forme $4n + 1$ et A de la forme $4n + 3$, $\mu$ est pairement ou impairement pair suivant que $a \equiv 1$ ou $5 \pmod{8}$. »

# MÉMOIRE

SUR

## L'ÉTUDE DES FONCTIONS DE PLUSIEURS QUANTITÉS,

SUR

## LA MANIÈRE DE LES FORMER

ET SUR

## LES SUBSTITUTIONS QUI LES LAISSENT INVARIABLES;

PAR M. ÉMILE MATHIEU.

Quand je me suis occupé de la question qui est traitée dans ce Mémoire, on ne connaissait alors de fonctions remarquables que la fonction deux fois transitive (ou résolvante) de Lagrange et une fonction trois fois transitive de 6 lettres ayant 6 valeurs donnée par M. Hermite; ajoutons à cela les deux fonctions deux fois transitives qui ont été rencontrées durant le cours de mes recherches par M. Kronecker, l'une de 7 lettres ayant 30 valeurs, l'autre de 11 lettres ayant 60480 valeurs, et l'on aura toutes les fonctions qui ont été données avant mes publications. Je rappellerai encore que, malgré le petit nombre de résultats acquis à cette doctrine, Cauchy avait publié pendant le cours de l'année 1845, dans les *Comptes rendus des séances de l'Académie*, une longue série de Mémoires entièrement relatifs à cette théorie, mais il ne fit la découverte d'aucune fonction.

A ces Mémoires de Cauchy j'ai toutefois emprunté une idée, et une seule : c'est celle de distinguer les fonctions en fonctions transitives et en fonctions intransitives. En effet, dans cette théorie, ce sont les fonctions transitives, et surtout celles qui le sont plusieurs fois, qui sont seules vraiment remarquables.

J'ai donné dans ce journal (année 1860) des notions générales sur les

fonctions transitives, et j'ai démontré l'existence de fonctions trois fois transitives de $p+1$ et de $p^r+1$ quantités, lorsque $p$ est un nombre premier.

Dans le Mémoire actuel je supposerai connus ces résultats et je n'y reviendrai pas; mais j'exposerai la découverte de plusieurs autres familles de fonctions plusieurs fois transitives dont le nombre des quantités est une puissance d'un nombre premier ou un tel nombre augmenté d'une unité, et je donnerai des méthodes très-simples pour les former. Et l'on comprendra toute l'importance de mes théorèmes, sachant qu'ayant cherché directement toutes les fonctions qui n'ont pas plus de 12 quantités, j'ai pu reconnaître que les 22 fonctions de moins de 11 quantités qui sont plusieurs fois transitives sont renfermées dans les familles que j'ai découvertes. Ce résultat fait voir clairement que l'on n'a pas de fonctions de $n$ quantités plusieurs fois transitives, lorsqu'on laisse le nombre $n$ complétement indéterminé, et ensuite que mes théorèmes donnent toutes les fonctions plusieurs fois transitives dont le nombre des variables est un nombre premier, une puissance d'un nombre premier, ou de tels nombres augmentés d'une unité, lorsqu'on ne particularise pas davantage le nombre des variables. Enfin, j'ai pu m'apercevoir qu'en particularisant convenablement ces mêmes nombres, on trouverait de certaines fonctions qui seraient invariables d'abord par les substitutions qui ne changent pas mes fonctions plusieurs fois transitives, et ensuite par un nombre plus ou moins grand d'autres substitutions. Je ne saurais mieux faire que de donner ici pour exemple l'étonnante fonction 5 fois transitive de 12 quantités que l'on trouvera dans ce Mémoire; cette fonction est due : 1° à ce que 12 est un nombre premier 11, augmenté d'une unité; 2° à ce que le nombre 11 est le double d'un nombre premier, plus 1; 3° à ce que 11 est une puissance paire d'un nombre premier, plus 2.

Ainsi je dois dire que, bien que les familles de fonctions que j'ai trouvées donnent les fonctions plusieurs fois transitives qui se présentent le plus ordinairement, je ne doute pas que par suite du concours de circonstances plus ou moins extraordinaires, il y ait non-seulement d'autres fonctions, mais encore qu'il y ait un nombre très-considérable de classes de fonctions plusieurs fois transitives, en ne rangeant dans une même classe que des fonctions dues à des circonstances identiques.

Ce Mémoire contient aussi une méthode qui permet de découvrir des fonctions plusieurs fois transitives, et des théorèmes généraux sur les fonctions transitives d'un nombre premier de quantités.

---

## CHAPITRE I.

### DE LA FORMATION DES FONCTIONS. — MÉTHODE POUR DÉCOUVRIR ET FORMER DES FONCTIONS PLUSIEURS FOIS TRANSITIVES.

#### *De la formation des fonctions.*

Considérons une fonction de $n$ quantités, que nous représenterons par la seule lettre $x$ affectée de $n$ indices différents; soit $\varphi(z)$ une fonction de $z$ telle, qu'en remplaçant $z$ par ces $n$ indices les résultats soient ces mêmes indices pris seulement dans un ordre différent; $\varphi(z)$ pourra caractériser une substitution que nous désignerons par $(x_z\, x_{\varphi z})$, ou même souvent par $(z, \varphi z)$.

D'après cela, soit

$$(1) \qquad (x_z\, x_z),\ (x_z\, x_{\varphi_1 z}),\ (x_z\, x_{\varphi_2 z}),\dots,\ (x_z\, x_{\varphi_{r-1} z})$$

un système de substitutions *conjuguées,* c'est-à-dire telles, qu'en faisant une quelconque de ces substitutions, puis cette même substitution ou une autre des substitutions (1), on fasse en définitive une des substitutions (1), on aura

$$\varphi_\alpha \varphi_\beta z = \varphi_\gamma z.$$

Théorème. — *Il y a toujours une fonction invariable par un système de substitutions conjuguées donné, et invariable par ces seules substitutions.*

Proposons-nous de former une fonction invariable par le système de substitutions conjuguées (1), et supposons que les indices des $n$ variables soient $0, 1, 2,\dots, n-1$. Soit

$$\psi(x_0,\ x_1,\ x_2,\dots,\ x_{n-1})$$

une fonction qui a $1.2.3\ldots n$ valeurs, et qui est par conséquent changée par toute substitution. Sur cette fonction faisons successivement toutes les substitutions (1), nous aurons les $r$ fonctions différentes :

$$(2)\quad \begin{cases} \psi(x_0, & x_1, & x_2,\ldots, & x_{n-1}), \\ \psi\left(x_{\varphi_1 0}, \right. & x_{\varphi_1 1}, & x_{\varphi_1 2},\ldots, & \left. x_{\varphi_1(n-1)}\right), \\ \psi\left(x_{\varphi_2 0}, \right. & x_{\varphi_2 1}, & x_{\varphi_2 2},\ldots, & \left. x_{\varphi_2(n-1)}\right), \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \psi\left(x_{\varphi_{r-1} 0}, \right. & x_{\varphi_{r-1} 1}, & x_{\varphi_{r-1} 2},\ldots, & \left. x_{\varphi_{r-1}(n-1)}\right). \end{cases}$$

Prenons une fonction symétrique de ces $r$ fonctions, et nous aurons une fonction $\Psi$ qui est invariable par les substitutions (1).

En effet, faisons sur les fonctions (2) la substitution $(z, \varphi_e z)$, elles deviendront

$$(3)\quad \begin{cases} \psi\left(x_{\varphi_e 0}, \right. & x_{\varphi_e 1}, & x_{\varphi_e 2},\ldots, & \left. x_{\varphi_e(n-1)}\right), \\ \psi\left(x_{\varphi_e\varphi_1 0}, \right. & x_{\varphi_e\varphi_1 1}, & x_{\varphi_e\varphi_1 2},\ldots, & \left. x_{\varphi_e\varphi_1(n-1)}\right), \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \psi\left(x_{\varphi_e\varphi_{r-1} 0}, \right. & x_{\varphi_e\varphi_{r-1} 1}, & x_{\varphi_e\varphi_{r-1} 2},\ldots, & \left. x_{\varphi_e\varphi_{r-1}(n-1)}\right). \end{cases}$$

Or on a $\varphi_e\varphi_g z = \varphi_v z$; d'ailleurs les fonctions (2) étant différentes, les fonctions (3) le sont aussi; donc les fonctions (3) sont les fonctions (2) prises dans un autre ordre; donc $\Psi$ est invariable par les substitutions (1). Il est évident qu'en général la fonction $\Psi$ est changée par toute autre substitution, et que le nombre de ses valeurs distinctes est $\frac{1.2.3\ldots n}{r}$.

Si, $\psi(x_0, x_1, x_2,\ldots, x_{n-1})$ étant une fonction quelconque, le nombre des valeurs de la fonction $\Psi$ n'était pas $\frac{1.2\ldots n}{r}$, il serait, comme il est aisé de le démontrer, un diviseur de ce nombre.

Supposons actuellement que $\psi(x_0, x_1, x_2,\ldots, x_{n-1})$ soit invariable par un système de substitutions conjuguées

$$(4)\qquad (z, z),\ (z, \theta_1 z),\ (z, \theta_2 z),\ldots,\ (z, \theta_{n-1} z).$$

Écrivons les substitutions

$$
(\mathrm{A})\quad \begin{cases}
(z, z), & (z, \theta_1 z), & (z, \theta_2 z), \ldots, & (z, \theta_{u-1} z), \\
(z, \varphi_1 z), & (z, \varphi_1 \theta_1 z), & (z, \varphi_1 \theta_2 z), \ldots & (z, \varphi_1 \theta_{u-1} z), \\
(z, \varphi_2 z), & (z, \varphi_2 \theta_1 z), & (z, \varphi_2 \theta_2 z), \ldots, & (z, \varphi_2 \theta_{u-1} z), \\
\ldots & \ldots & \ldots & \ldots \\
(z, \varphi_{r-1} z), & (z, \varphi_{r-1} \theta_1 z), & (z, \varphi_{r-1} \theta_2 z), \ldots, & (z, \varphi_{r-1} \theta_{u-1} z).
\end{cases}
$$

Si la réunion de ces substitutions forme un système de substitutions conjuguées, je dis que la fonction $\Psi$, formée comme il a été dit ci-dessus, est invariable par ce système de substitutions.

La fonction $\Psi$ est encore invariable par les substitutions (1); il reste donc à démontrer qu'elle n'est pas changée non plus par les substitutions (4). Sur la fonction $\Psi$ faisons la substitution $(z, \theta_e z)$, les fonctions (2) qui la composent deviendront

$$
(6)\quad \begin{cases}
\psi\left(x_{\theta_e 0}, \quad x_{\theta_e 1}, \quad x_{\theta_e 2}, \ldots, \quad x_{\theta_e (n-1)}\right), \\
\psi\left(x_{\theta_e \varphi_1 0}, \; x_{\theta_e \varphi_1 1}, \; x_{\theta_e \varphi_1 2}, \ldots, \; x_{\theta_e \varphi_1 (n-1)}\right), \\
\psi\left(x_{\theta_e \varphi_2 0}, \; x_{\theta_e \varphi_2 1}, \; x_{\theta_e \varphi_2 2}, \ldots, \; x_{\theta_e \varphi_2 (n-1)}\right), \\
\ldots\ldots\ldots\ldots\ldots\ldots
\end{cases}
$$

La substitution $(z, \theta_e \varphi_s z)$ fait partie du système de substitutions conjuguées (A), puisqu'on l'obtient en faisant $(z, \varphi_s z)$, puis $(z, \theta_e z)$; donc on a

$$
\theta_e \varphi_s z = \varphi_\alpha \theta_\beta z.
$$

Ainsi les fonctions (6) peuvent s'écrire

$$
(7)\quad \begin{cases}
\psi\left(x_{\theta_e 0}, \qquad x_{\theta_e 1}, \qquad x_{\theta_e 2}, \ldots, \qquad x_{\theta_e (n-1)}\right), \\
\psi\left(x_{\varphi_{\alpha_1} \theta_{\beta_1} 0}, \quad x_{\varphi_{\alpha_1} \theta_{\beta_1} 1}, \quad x_{\varphi_{\alpha_1} \theta_{\beta_1} 2}, \ldots, \quad x_{\varphi_{\alpha_2} \theta_{\beta_1} (n-1)}\right), \\
\ldots\ldots\ldots\ldots\ldots\ldots \\
\psi\left(x_{\varphi_{\alpha_{r-1}} \theta_{\beta_{r-1}} 0}, \; x_{\varphi_{\alpha_{r-1}} \theta_{\beta_{r-1}} 1}, \ldots, \; x_{\varphi_{\alpha_{r-1}} \theta_{\beta_{r-1}} (n-1)}\right).
\end{cases}
$$

La première des fonctions (2) est invariable par la substitution $(z, \theta_e z)$; donc elle est égale à la première des fonctions (7). On voit aussi, par la même raison, que la seconde des fonctions (7) est égale à

$$\psi\left(x_{\varphi_{\alpha_1} 0}, x_{\varphi_{\alpha_1} 1}, x_{\varphi_{\alpha_1} 2}, \ldots, x_{\varphi_{\alpha_1} (n-1)}\right),$$

que la troisième des fonctions (7) est égale à

$$\psi\left(x_{\varphi_{\alpha_2} 0}, x_{\varphi_{\alpha_2} 1}, x_{\varphi_{\alpha_2} 2}, \ldots, x_{\varphi_{\alpha_2} (n-1)}\right),$$

et ainsi des autres. Donc les fonctions (7) sont les fonctions (2) prises dans un autre ordre; car il est clair qu'elles sont différentes entre elles et la fonction $\Psi$ est invariable par le système des substitutions (4); donc enfin $\Psi$ est invariable par le système des substitutions conjuguées (A).

Le système des substitutions conjuguées (A) peut aussi s'écrire :

$$\left\{\begin{array}{llll}
(z, z), & (z, \varphi_1 z); & (z, \varphi_2 z), \ldots, & (z, \varphi_{r-1} z), \\
(z, \theta_1 z), & (z, \theta_1 \varphi_1 z), & (z, \theta_1 \varphi_2 z), \ldots, & (z, \theta_1 \varphi_{r-1} z), \\
\ldots & \ldots & \ldots & \ldots \\
(z, \theta_{u-1} z), & (z, \theta_{u-1} \varphi_1 z), & (z, \theta_{u-1} \varphi_2 z), \ldots, & (z, \theta_{u-1} \varphi_{r-1} z);
\end{array}\right.$$

car toutes ces substitutions sont différentes. Supposons en effet que l'on ait

$$\theta_s \varphi_r z = \theta_v \varphi_t z;$$

désignons par $\theta'_s z$ et $\varphi'_t z$ les fonctions inverses de $\theta_s z$ et de $\varphi_t z$, nous aurons

$$\varphi_r z = \theta'_s \theta_v \varphi_t z \quad \text{et} \quad \varphi_r \varphi'_t z = \theta'_s \theta_v z,$$

et l'une des substitutions (1) serait identique à une des substitutions (4), ce qui ne doit pas avoir lieu.

D'après cela, on peut encore former une fonction invariable par le système des substitutions conjuguées (A) de la manière suivante. On formera d'abord la fonction

$$\chi(x_0, x_1, x_2, \ldots, x_{n-1}),$$

qui soit invariable par le système de substitutions conjuguées (1); puis sur cette fonction on fera toutes les substitutions (4); enfin on prendra une fonction symétrique X des fonctions ainsi obtenues.

Il est évident que les fonctions (2) sont invariables respectivement par les systèmes suivants de substitutions conjuguées :

$$(z, z), \quad (z, \theta_1 z), \quad (z, \theta_2 z), \ldots, \quad (z, \theta_{u-1} z);$$
$$(\varphi_1 z, \varphi_1 z), \quad (\varphi_1 z, \varphi_1 \theta_1 z), \quad (\varphi_1 z, \varphi_1 \theta_2 z), \ldots, \quad (\varphi_1 z, \varphi_1 \theta_{u-1} z);$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(\varphi_{r-1} z, \varphi_{r-1} z), \quad (\varphi_{r-1} z, \varphi_{r-1} \theta_1 z), \quad (\varphi_{r-1} z, \varphi_{r-1} \theta_2 z), \ldots, \quad (\varphi_{r-1} z, \varphi_{r-1} \theta_{u-1} z),$$

et si on désigne en général par $\varphi'_e z$ la fonction inverse de $\varphi_e z$, ces systèmes de substitutions peuvent s'écrire

$$(z, z), \quad (z, \theta_1 z), \quad (z, \theta_2 z), \ldots, \quad (z, \theta_{u-1} z),$$
$$(z, z), \quad (z, \varphi_1 \theta_1 \varphi'_1 z), \quad (z, \varphi_1 \theta_2 \varphi'_1 z), \ldots, \quad (z, \varphi_1 \theta_{u-1} \varphi'_1 z),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(z, z), \quad (z, \varphi_{r-1} \theta_1 \varphi'_{r-1} z), \quad (z, \varphi_{r-1} \theta_2 \varphi'_{r-1} z), \ldots, \quad (z, \varphi_{r-1} \theta_{u-1} \varphi'_{r-1} z).$$

*Méthode pour former des fonctions plusieurs fois transitives.*

Soit une fonction transitive F de $n$ quantités $x_0, x_1, x_2, \ldots, x_{n-1}$, qui, considérée comme fonction des $n - 1$ quantités $x_1, x_2, \ldots, x_{n-1}$, est invariable par le système des substitutions conjuguées

$$(1) \qquad (x_z x_z), \quad \left(x_z x_{\theta_1 z}\right), \quad \left(x_z x_{\theta_2 z}\right), \ldots, \quad \left(x_z x_{\theta_{r-1} z}\right),$$

et qui n'est pas changée non plus par les $n - 1$ substitutions

$$(2) \qquad \left(x_z x_{\varphi_1 z}\right), \quad \left(x_z x_{\varphi_2 z}\right), \ldots, \quad \left(x_z x_{\varphi_{n-1} z}\right),$$

qui s'effectuent sur toutes les $n$ variables, et qui jointes à $(x_z x_z)$ constituent un système de substitutions conjuguées qui caractérise une fonction transitive. Nous nous proposons de former, si elle existe, une fonction deux fois transitive $\Phi$ des $n + 1$ variables $x_0, x_1, x_2, \ldots,$

$x_{n-1}$, $x_0$, qui, considérée comme fonction des $n$ premières variables, soit semblable à F.

Considérée comme fonction des $n-1$ variables $x_1, x_2, \ldots, x_{n-1}$, la fonction $\Phi$ n'est pas changée par les substitutions (1). Si donc on désigne dans un ordre convenable les variables $x_1, x_2, \ldots, x_{n-1}$ par $x'_1, x'_2, \ldots, x'_{n-1}$, par la raison que $\Phi$ n'est pas changée par les substitutions (1) et (2), $\Phi$ considérée comme fonction des variables $x'_0$, $x'_1$, $x'_2, \ldots, x'_{n-1}$ n'est pas changée par les substitutions

$$(3) \qquad (x'_z x'_z), \quad \left(x'_z x'_{\theta_1 z}\right), \quad \left(x'_z x'_{\theta_2 z}\right), \ldots, \quad \left(x'_z x'_{\theta_{r-1} z}\right),$$

$$(4) \qquad \left(x'_z x'_{\varphi_1 z}\right), \quad \left(x'_z x'_{\varphi_2 z}\right), \ldots, \quad \left(x'_z x'_{\varphi_{n-1} z}\right).$$

Or les substitutions (1) et les substitutions (3) s'effectuent sur les mêmes variables $x_1, x_2, \ldots, x_{n-1}$; donc elles sont identiques. Quant aux substitutions (4), elles contiennent les $n$ variables $x'_0$, $x_1$, $x_2, \ldots, x_{n-1}$, et si la valeur de chaque $x'$ était connue, une quelconque des substitutions (4), jointe aux substitutions (1) et (2), suffirait pour que l'on pût former le système de toutes les substitutions conjuguées qui laissent $\Phi$ invariable. Or, les substitutions (3) étant identiques aux substitutions (1), une quelconque des substitutions (3) $\left(x'_z x'_{\theta_\beta z}\right)$ est identique à une certaine substitution (1) $\left(x_z x_{\theta_\alpha z}\right)$ qui lui est semblable. Supposons qu'en identifiant ces deux substitutions on trouve $x'_z = x_{\chi z}$; on aura les substitutions (4) en remplaçant les $x'$ par leurs valeurs.

D'après cela, pour obtenir des substitutions qui laissent invariable la fonction $\Phi$ et qui contiennent $x'_0$, on choisira parmi les substitutions (1) celle qui renferme le moins de cycles, une substitution circulaire, s'il y en a une. Soit $\left(x_z x_{\theta_\alpha z}\right)$ cette substitution; on identifiera cette substitution de toutes les manières possibles avec chacune des substitutions (3) qui lui seront semblables. Restera ensuite à reconnaître celles de ces identifications qui sont bonnes, et pour cela on cherchera si, parmi les substitutions dérivées des substitutions (1), (2) et (4), il y en a qui s'effectuent sur les $n$ variables $x_0, x_1, x_2, \ldots, x_{n-1}$, et qui ne coïncident pas avec les substitutions (1) et (2); dans quel cas l'identification est à rejeter. Mais si l'identification est reconnue bonne,

on pourra former le système de substitutions conjuguées qui laissent $\Phi$ invariable, et par suite former $\Phi$.

Si dans les substitutions (1) toutes les variables entrent de la même manière, ce qui aura lieu en particulier si la fonction F est deux fois transitive, et par suite la fonction $\Phi$ trois fois transitive, on pourra poser $x'_1 = x_1$ ; ce qui facilitera beaucoup l'identification de la substitution $\left(x_z x_{\theta_\alpha z}\right)$ avec chacune des substitutions (3) qui lui sont semblables ; ainsi, par exemple, si $\left(x_z x_{\theta_\alpha z}\right)$ est une substitution circulaire de $n-1$ variables, il n'y aura qu'une seule manière de l'identifier avec une substitution (3) qui lui est semblable, au lieu qu'il y en ait $n$.

Si la fonction $\Phi$ était quatre fois transitive, on pourrait non-seulement faire $x'_1 = x_1$, mais on pourrait poser $x'_e = x_f$. Si la fonction $\Phi$ était cinq fois transitive, on pourrait faire

$$x'_1 = x_1, \quad x'_e = x_f, \quad x'_g = x_h.$$

Nous allons maintenant nous proposer de former la fonction $\Phi$.

La fonction

$$\mathrm{F} = \mathrm{F}(x_0, x_1, x_2, \ldots, x_{n-1})$$

est invariable par le système de substitutions conjuguées :

$$(\mathrm{A}) \quad \begin{cases} (x_z x_z), \ \left(x_z x_{\theta_1 z}\right), \ldots, \left(x_z x_{\theta_{r-1} z}\right), \ \left(x_z x_{\varphi_1 z}\right), \ \left(x_z x_{\varphi_1 \theta_1 z}\right), \ldots, \\ \left(x_z x_{\varphi_{n-1} \theta_{r-1} z}\right). \end{cases}$$

Remarquons ensuite que, puisque l'on a $x'_z = x_{\chi z}$, une quelconque des substitutions (4) $\left(x'_z x'_{\varphi_r z}\right)$ peut s'écrire $\left(x_{\chi z} x_{\chi \varphi_r z}\right)$ ou $\left(x_z x_{\chi \varphi_r \chi' z}\right)$, en désignant par $\chi' z$ la fonction inverse de $\chi z$, ou enfin $\left(x_z x_{\varphi'_r z}\right)$ en posant

$$\chi \varphi_r \chi' z = \varphi'_r z.$$

La fonction $\Phi$ est donc évidemment invariable par les $rn^2$ substitu-

tions suivantes :

$$
(\mathrm{B})\quad \left\{
\begin{array}{l}
\left[\begin{array}{llll}
(x_z x_z), & (x_z x_{\theta_1 z}),\ldots, & (x_z x_{\theta_{r-1} z}), \\
(x_z x_{\varphi_1 z}), & (x_z x_{\varphi_1\theta_1 z}),\ldots, & (x_z x_{\varphi_{n-1}\theta_{r-1} z}).
\end{array}\right] \\
\left[\begin{array}{llll}
(x_z x_{\varphi'_1 z}), & (x_z x_{\varphi'_1\theta_1 z}),\ldots, & (x_z x_{\varphi'_1\theta_{r-1} z}), \\
(x_z x_{\varphi'_1\varphi_1 z}), & (x_z x_{\varphi'_1\varphi_1\theta_1 z}),\ldots, & (x_z x_{\varphi'_1\varphi_{n-1}\theta_{r-1} z}),
\end{array}\right] \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\left[\begin{array}{llll}
(x_z x_{\varphi'_{n-1} z}), & (x_z x_{\varphi'_{n-1}\theta_1 z}),\ldots, & (x_z x_{\varphi'_{n-1}\theta_{r-1} z}), \\
(x_z x_{\varphi'_{n-1}\varphi_1 z}), & (x_z x_{\varphi'_{n-1}\varphi_1\theta_1 z}),\ldots, & (x_z x_{\varphi'_{n-1}\varphi_{n-1}\theta_{r-1} z}).
\end{array}\right]
\end{array}\right.
$$

Toutes ces substitutions sont différentes ; car si, en désignant les fonctions $\varphi\theta z$ par $\psi z$, on avait

$$\varphi'_r\psi_s z = \varphi_\alpha\psi_\beta z,$$

on aurait, en désignant par $\varphi'_{\alpha_1}$ l'inverse de $\varphi'_\alpha$,

$$\varphi'_{\alpha_1}\varphi'_r\psi_s z = \psi_\beta z,$$

et en changeant $z$ en $\psi_{s_1} z$, inverse de $\psi_s z$,

$$\varphi'_{\alpha_1}\varphi'_r z = \psi_\beta\psi_{s_1} z,$$

égalité impossible puisque $(x_z x_{\varphi'_{\alpha_1}\varphi'_r z})$ permute nécessairement $x_z$, et que $(x_z x_{\psi_\beta\psi_{s_1} z})$ ne le permute pas.

Ainsi il reste $rn$ substitutions à ajouter aux substitutions (B) pour compléter le système des $rn(n+1)$ substitutions conjuguées qui laissent $\Phi$ invariable. Désignons par $(x_z x_{\lambda z})$ une quelconque de ces $rn$ substitutions, ces $rn$ substitutions seront

$$
(\mathrm{C})\quad \left[\begin{array}{llll}
(x_z x_{\lambda z}), & (x_z x_{\lambda\theta_1 z}),\ldots, & (x_z x_{\lambda\theta_{r-1} z}), \\
(x_z x_{\lambda\varphi_1 z}), & (x_z x_{\lambda\varphi_1\theta_1 z}),\ldots, & (x_z x_{\lambda\varphi_{n-1}\theta_{r-1} z}),
\end{array}\right]
$$

car elles sont distinctes entre elles et elles sont distinctes des substitutions (B), comme on le voit aisément.

Aucune des substitutions (B) ne change $x'_0$ en $x_0$; donc les $m$ substitutions (C) changent $x'_0$ en $x_0$. Supposons que $(x_z x_{\varphi_1 z})$ change $x_0$ en $x_1$; représentons l'inverse de $\varphi_1 z$ par $\varphi_{-1} z$; supposons aussi que l'on ait $x'_1 = x_1$ et alors $(x_z x_{\varphi'_1 z})$ change $x'_0$ en $x_1$ et $(x_z x_{\varphi_{-1} z})$ change $x_1$ en $x_0$; donc la substitution

$$\left(x_z x_{\varphi_{-1}\varphi'_1 z}\right)$$

change $x_0'$ en $x_0$, et peut être prise pour la substitution $(x_z x_{\lambda z})$.

Cela posé, formons les fonctions

$$(D)\quad \begin{cases} F\left(x_0, & x_1, & x_2, \ldots, & x_{(n-1)}\right), \\ F\left(x_{\varphi'_1 0}, & x_{\varphi'_1 1}, & x_{\varphi'_1 2}, \ldots, & x_{\varphi'_1 (n-1)}\right), \\ \ldots & \ldots & \ldots & \ldots \\ F\left(x_{\varphi'_{n-1} 0}, & x_{\varphi'_{n-1} 1}, & x_{\varphi'_{n-1} 2}, \ldots, & x_{\varphi'_{n-1}(n-1)}\right), \\ F\left(x_{\lambda 0}, & x_{\lambda 1}, & x_{\lambda 2}, \ldots, & x_{\lambda (n-1)}\right), \end{cases}$$

que l'on obtient en faisant sur la première les substitutions (4), puis $(x_z x_{\lambda z})$. Prenons une fonction $\Theta$ symétrique des $n+1$ fonctions (D), et nous allons démontrer que la fonction $\Theta$ est invariable par les substitutions (B) et (C), et par conséquent n'est autre que la fonction $\Phi$.

En effet, soit $(x_z x_{\psi z})$ une quelconque des substitutions (B) et (C), et démontrons que $\Theta$ n'est pas changée par cette substitution.

Considérons une quelconque des fonctions (D)

$$(K)\qquad F\left(x_{\varphi'_\alpha 0}, x_{\varphi'_\alpha 1}, x_{\varphi'_\alpha 2}, \ldots, x_{\varphi'_\alpha (n-1)}\right);$$

la substitution $(x_z x_{\psi z})$ changera cette fonction en la suivante

$$(E)\qquad F\left(x_{\psi\varphi'_\alpha 0}, x_{\psi\varphi'_\alpha 1}, x_{\psi\varphi'_\alpha 2}, \ldots, x_{\psi\varphi'_\alpha (n-1)}\right).$$

La substitution $\left(x_z x_{\psi\varphi'_\alpha z}\right)$ fait nécessairement partie des substitutions (B) et (C); on a donc

$$\psi\varphi'_\alpha z = \varphi'_a \varphi_c \theta_b z \quad \text{ou} \quad \psi\varphi'_\alpha z = \lambda\varphi_c\theta_b z.$$

Dans le premier de ces deux cas, la fonction (E) peut s'écrire

$$F\left(x_{\varphi'_a\varphi_c\theta_b 0}, x_{\varphi'_a\varphi_c\theta_b 1}, \ldots, x_{\varphi'_a\varphi_c\theta_b(n-1)}\right);$$

or la fonction $F(x_0, x_1, \ldots, x_{n-1})$ est invariable par la substitution $(x_z\, x_{\varphi_c\theta_b z})$; donc la fonction (E) peut encore s'écrire

$$F\left(x_{\varphi'_a 0}, x_{\varphi'_a 1}, \ldots, x_{\varphi'_a(n-1)}\right),$$

et c'est une des fonctions (D). Dans le deuxième cas, la fonction (E) peut s'écrire

$$F\left(x_{\lambda\varphi_c\theta_b 0}, x_{\lambda\varphi_c\theta_b 1}, \ldots, x_{\lambda\varphi_c\theta_b(n-1)}\right),$$

ou encore

$$F(x_{\lambda 0}, x_{\lambda 1}, \ldots, x_{\lambda(n-1)}).$$

Donc la substitution $(x_z\, x_{\psi z})$ change la fonction (K) en une autre fonction (D). Ce que nous venons de dire de la fonction (K) est applicable à une quelconque des fonctions (D), y compris la dernière.

D'ailleurs les fonctions (D) étant toutes différentes le sont encore après que l'on a fait sur elles la substitution $(x_z\, x_{\psi z})$; donc cette dernière ne fait que permuter les fonctions (D).

*Application.* — Considérons une fonction F de sept quantités $x_0, x_1, \ldots, x_6$ qui soit invariable par les seules substitutions $(x_z\, x_{a^2z+b})$; regardée comme fonction des six variables $x_1, x_2, \ldots, x_6$ seulement, cette fonction n'est invariable que par les substitutions $(x_z\, x_{a^2z})$, c'est-à-dire par

$$(e) \qquad (x_1 x_2 x_4)(x_3 x_6 x_5) \quad \text{et} \quad (x_1 x_4 x_2)(x_3 x_5 x_6),$$

et les substitutions de sept variables qui ne la changent pas, sont les puissances de $(x_z\, x_{z+1})$ ou de

$$(d) \qquad (x_0 x_1 x_2 x_3 x_4 x_5 x_6).$$

Le nombre des valeurs de cette fonction transitive est

$$\frac{1.2.3.4.5.6}{3} = 240.$$

Cela posé, cherchons s'il existe une fonction deux fois transitive des huit quantités $x_0$, $x_1, \ldots, x_6\, x'_0$, et qui, considérée comme fonction des sept premières, soit semblable à F.

En désignant les quantités $x_1, x_2, \ldots, x_6$ dans un ordre convenable par $x'_1, x'_2, \ldots, x'_6$, cette fonction deux fois transitive sera invariable par les substitutions

$$(e') \qquad (x'_1\, x'_2\, x'_4)(x'_3\, x'_6\, x'_5) \quad \text{et} \quad (x'_1\, x'_4\, x'_2)(x'_3\, x'_6\, x'_5),$$

et par les puissances de la substitution

$$(d') \qquad (x'_0\, x'_1\, x'_2\, x'_3\, x'_4\, x'_5\, x'_6).$$

Les substitutions $(e)$ sont identiques aux substitutions $(e')$. Faisons

$$x'_1 = x_1.$$

En identifiant la première des substitutions $(e)$ avec la première des substitutions $(e')$, on aura les deux résultats suivants :

1° $x'_1 = x_1$, $x'_2 = x_2$, $x'_4 = x_4$, $x'_3 = x_6$, $x'_6 = x_5$, $x'_5 = x_3$;

2° $x'_1 = x_1$, $x'_2 = x_2$, $x'_4 = x_4$, $x'_3 = x_5$, $x'_6 = x_3$, $x'_5 = x_6$.

On pourra ensuite identifier la première des substitutions $(e)$ avec la seconde des substitutions $(e')$ d'une des trois manières suivantes :

3° $x'_1 = x_1$, $x'_4 = x_2$, $x'_2 = x_4$, $x'_3 = x_3$, $x'_5 = x_6$, $x'_6 = x_5$;

4° $x'_1 = x_1$, $x'_4 = x_2$, $x'_2 = x_4$, $x'_3 = x_6$, $x'_5 = x_5$, $x'_6 = x_3$;

5° $x'_1 = x_1$, $x'_4 = x_2$, $x'_2 = x_4$, $x'_3 = x_5$, $x'_5 = x_3$, $x'_6 = x_6$.

D'après cela, la substitution $(d')$ sera l'une des cinq suivantes :

$$(1) \qquad (x'_0\, x_1\, x_2\, x_6\, x_4\, x_3\, x_5),$$

$$(2) \qquad (x'_0\, x_1\, x_2\, x_5\, x_4\, x_6\, x_3),$$

$$(3) \qquad (x'_0\, x_1\, x_4\, x_3\, x_2\, x_6\, x_5),$$

$$(4) \qquad (x'_0\, x_1\, x_4\, x_6\, x_2\, x_5\, x_3),$$

$$(5) \qquad (x'_0\, x_1\, x_4\, x_5\, x_2\, x_3\, x_6).$$

La substitution (3) ne peut convenir; en effet faisons la substitution ($d$), puis la substitution (3), opération représentée par le tableau

$$\begin{array}{cccccccc} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x'_0 \\ x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_0 & x'_0 \\ x_4 & x_6 & x_2 & x_3 & x'_0 & x_5 & x_0 & x_1 \end{array}$$

et nous aurons la substitution $(x_0\, x_4\, x'_0\, x_1\, x_6)$ qui ne peut laisser invariable la fonction cherchée, puisqu'elle n'est semblable ni aux substitutions ($e$), ni à la substitution ($d$).

La quatrième identification ne peut convenir non plus; en effet faisons la substitution (4), puis deux fois la substitution ($d$), ce qui est indiqué par le tableau

$$\begin{array}{cccccccc} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x'_0 \\ x_0 & x_4 & x_5 & x'_0 & x_6 & x_3 & x_2 & x_1 \\ x_2 & x_6 & x_0 & x'_0 & x_1 & x_5 & x_4 & x_3 \end{array}$$

et nous aurons la substitution $(x_0\, x_2)\, (x_1\, x_6\, x_4)\, (x_3\, x'_0)$, qui ne peut laisser invariable la fonction cherchée.

Reste donc à examiner s'il existe des fonctions transitives de huit quantités ayant 240 valeurs, invariables par l'un des trois systèmes de substitutions suivants

1° $(x_1\, x_2\, x_4)\, (x_3\, x_6\, x_5)$, $(x_0\, x_1\, x_2\, x_3\, x_4\, x_5\, x_6)$, $(x'_0\, x_1\, x_2\, x_6\, x_4\, x_3\, x_5)$;

2° $(x_1\, x_2\, x_4)\, (x_3\, x_6\, x_5)$, $(x_0\, x_1\, x_2\, x_3\, x_4\, x_5\, x_6)$, $(x'_0\, x_1\, x_2\, x_5\, x_4\, x_6\, x_3)$;

3° $(x_1\, x_2\, x_4)\, (x_3\, x_6\, x_5)$, $(x_0\, x_1\, x_2\, x_3\, x_4\, x_5\, x_6)$, $(x'_0\, x_1\, x_4\, x_5\, x_2\, x_3\, x_6)$.

Si sur le premier système, on fait la substitution $(x_1\, x_6)$, $(x_2\, x_5)$, $(x_3\, x_4)$, il devient

$$(x_6\, x_5\, x_3)\, (x_4\, x_1\, x_2),\ (x_0\, x_6\, x_5\, x_4\, x_3\, x_2\, x_1),\ (x'_0\, x_6\, x_5\, x_1\, x_3\, x_4\, x_2);$$

les deux dernières de ces substitutions sont des puissances des deux dernières du système 2°; donc le système 2° ne diffère du système 1° que par la manière de désigner les variables.

Enfin si l'on cherche des substitutions dérivées du système 1° ou du système 3°, on ne trouve pas de substitutions de moins de huit quantités qui ne soient pas de la forme des substitutions ($e$) et ($d$). Il nous serait très-facile de former ici ces deux fonctions d'après ce qui a été dit ci-dessus; mais comme nous n'avons donné cette application que pour mieux faire comprendre notre méthode, nous ne nous arrêterons pas davantage sur ces deux fonctions [*].

Actuellement, conservant les notations employées ci-dessus, supposons qu'il y ait une fonction $\Phi$ au mois deux fois transitive de $n+1$ variables $x_0, x_1, x_2,\ldots, x_{n-1}, x'_0$ qui, considérée comme fonction des $n-1$ quantités $x_1, x_2,\ldots, x_{n-1}$ soit invariable par le système de substitutions conjuguées

$$(1)\qquad (x_z x_z),\ \left(x_z x_{\theta_1 z}\right),\ \left(x_z x_{\theta_2 z}\right),\ldots,\ \left(x_z x_{\theta_{r-1} z}\right),$$

et qui ne soit pas changée non plus par les $n-1$ substitutions

$$(2)\qquad \left(x_z x_{\varphi_1 z}\right),\ \left(x_z x_{\varphi_2 z}\right),\ \left(x_z x_{\varphi_3 z}\right),\ldots,\ \left(x_z x_{\varphi_{n-1} z}\right),$$

qui s'effectuent sur les $n$ variables, et au moyen desquelles on peut amener une quelconque des variables à la place d'une autre. Enfin la fonction $\Phi$ est invariable par les substitutions

$$(3)\qquad (x'_z x'_z),\quad \left(x'_z x'_{\theta_1 z}\right),\ \left(x'_z x'_{\theta_2 z}\right),\ldots,\ \left(x'_z x'_{\theta_{r-1} z}\right),$$

$$(4)\qquad \left(x'_z x'_{\varphi_1 z}\right),\ \left(x'_z x'_{\varphi_2 z}\right),\ \ldots\ldots\ldots,\ \left(x'_z x'_{\varphi_{n-1} z}\right),$$

les substitutions (3) étant identiques aux substitutions (1) dans un certain ordre. Supposons que l'identification des substitutions (3) avec les substitutions (1) ait donné $x'_z = x_{\chi z}$, nous aurons

$$\chi\theta_s\chi' z = \theta_v z,\quad \chi\varphi_r\chi' z = \varphi'_r z,\quad \chi\varphi_r\theta_s\chi' z = \varphi'_r\theta_v z,$$

[*] Nous reverrons ces deux fonctions dans le chapitre III à propos de la fonction de huit quantités qui a trente valeurs.

et la fonction $\Phi$ est invariable par les $rn(n+1)$ substitutions

$$
(B)\left\{
\begin{array}{l}
\left[\begin{array}{llll}
(x_z x_z), & (x_z x_{\theta_1 z}), & (x_z x_{\theta_2 z}), & (x_z x_{\theta_{r-1} z}), \\
 & (x_z x_{\varphi_1 z}), & (x_z x_{\varphi_1 \theta_1 z}), \ldots, & (x_z x_{\varphi_{n-1} \theta_{r-1} z}),
\end{array}\right] \\
\left[\begin{array}{llll}
(x_z x_{\varphi'_1 z}), & (x_z x_{\varphi'_1 \theta_1 z}), & (x_z x_{\varphi'_1 \theta_2 z}), \ldots, & (x_z x_{\varphi'_1 \theta_{r-1} z}), \\
 & (x_z x_{\varphi'_1 \varphi_1 z}), & (x_z x_{\varphi'_1 \varphi_1 \theta_1 z}), \ldots, & (x_z x_{\varphi'_1 \varphi_{n-1} \theta_{r-1} z}),
\end{array}\right] \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\left[\begin{array}{llll}
(x_z x_{\varphi'_{n-1} z}), & (x_z x_{\varphi'_{n-1} \theta_1 z}), & (x_z x_{\varphi'_{n-1} \theta_2 z}), \ldots, & (x_z x_{\varphi'_{n-1} \theta_{r-1} z}), \\
 & (x_z x_{\varphi'_{n-1} \varphi_1 z}), & (x_z x_{\varphi'_{n-1} \varphi_1 \theta_1 z}), \ldots, & (x_z x_{\varphi'_{n-1} \varphi_{n-1} \theta_{r-1} z}),
\end{array}\right]
\end{array}\right.
$$

$$
(C)\quad \left[\begin{array}{llll}
(x_z x_{\varphi_{-1} \varphi'_1 z}), & (x_z x_{\varphi_{-1} \varphi'_1 \theta_1 z}), & (x_z x_{\varphi_{-1} \varphi'_1 \theta_2 z}), \ldots, & (x_z x_{\varphi_{-1} \varphi'_1 \theta_{r-1} z}), \\
 & & (x_z x_{\varphi_{-1} \varphi'_1 \varphi_1 z}), \ldots, & (x_z x_{\varphi_{-1} \varphi'_1 \varphi'_{n-1} \theta_{r-1} z}),
\end{array}\right]
$$

$\varphi_{-1} z$ étant la fonction inverse de $\varphi_1 z$.

Supposons ensuite qu'il y ait une seconde identification des substitutions (3) avec les substitutions (1) qui donne une fonction semblable à la fonction $\Phi$, en faisant abstraction de la manière de désigner les variables. Au lieu des substitutions (3) et (4), nous aurons les substitutions

$$
(3') \qquad (x''_z x''_z), \quad (x''_z x''_{\theta_1 z}), \; (x''_z x''_{\theta_2 z}), \ldots, \; (x''_z x''_{\theta_{r-1} z}).
$$

$$
(4') \qquad (x''_z x''_{\varphi_1 z}), \; (x'_z x''_{\varphi_2 z}), \; \ldots\ldots, \; (x''_z x''_{\varphi_{n-1} z});
$$

les substitutions (3′) sont, dans un certain ordre, les substitutions (1), et on a $x''_z = x_{\mu z}$; posons

$$\mu \theta_s \mu' z = \theta_u z,$$

$$\mu \varphi_r \mu' z = \varphi''_r z,$$

par suite

$$\mu \varphi_r \theta_s \mu' z = \varphi''_r \theta_u z,$$

$\mu' z$ étant la fonction inverse de $\mu z$. Nous aurons donc le système de

substitutions conjuguées

$$(\mathrm{B}')\left\{\begin{array}{l}
\left[\begin{array}{llll}
(x_z x_z), & (x_z x_{\theta_1 z}), & (x_z x_{\theta_2 z}),\ldots, & (x_z x_{\theta_{r-1} z}),\\
 & (x_z x_{\varphi_1 z}), & (x_z x_{\varphi_1\theta_1 z}),\ldots, & (x_z x_{\varphi_{n-1}\theta_{r-1} z}),
\end{array}\right]\\
\left[\begin{array}{llll}
(x_z x_{\varphi''_1 z}), & (x_z x_{\varphi''_1\theta_1 z}), & (x_z x_{\varphi''_1\theta_2 z}),\ldots, & (x_z x_{\varphi''_1\theta_{r-1} z}),\\
 & (x_z x_{\varphi''_1\varphi_1 z}), & (x_z x_{\varphi''_1\varphi_1\theta_1 z}),\ldots, & (x_z x_{\varphi''_1\varphi_{n-1}\theta_{r-1} z}),
\end{array}\right]\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\left[\begin{array}{llll}
(x_z x_{\varphi''_{n-1} z}), & (x_z x_{\varphi''_{n-1}\theta_1 z}), & (x_z x_{\varphi''_{n-1}\theta_2 z}),\ldots, & (x_z x_{\varphi''_{n-1}\theta_{r-1} z}),\\
 & & (x_z x_{\varphi''_{n-1}\varphi_1 z}),\ldots, & (x_z x_{\varphi''_{n-1}\varphi_{n-1}\theta_{r-1} z}),
\end{array}\right]
\end{array}\right.$$

$$(\mathrm{C}')\quad\left[\begin{array}{lll}
(x_z x_{\varphi_{-1}\varphi''_1 z}), & (x_z x_{\varphi_{-1}\varphi''_1\theta_1 z}),\ldots, & (x_z x_{\varphi_{-1}\varphi''_1\theta_{r-1} z}),\\
 & (x_z x_{\varphi_{-1}\varphi''_1\varphi_1 z})\ldots, & (x_z x_{\varphi_{-1}\varphi''_1\varphi_{n-1}\theta_{r-1} z}),
\end{array}\right]$$

et, d'après l'hypothèse, le système (B′), (C′) ne diffère du système (B), (C) que par la manière de désigner les variables.

Supposons alors que l'on ait, $\tau' z$ étant l'inverse de $\tau z$,

$$\tau\theta_s\tau' z = \theta_e z,\quad \tau\varphi_\nu\tau' z = \varphi_f z,\quad \tau\varphi'_\alpha\tau' z = \varphi''_\beta z;$$

nous aurons

$$\tau\varphi'_\alpha\varphi_\nu\theta_s\tau' z = \varphi''_\beta\varphi_f\theta_e z;$$

on passera donc des substitutions (B) aux substitutions (B′) par la substitution $(x_z x_{\tau z})$; par suite la substitution $(x_z x_{\tau\varphi_{-1}\varphi'_1\tau' z})$ est une des substitutions (C′) et on peut poser

$$\tau\varphi_{-1}\varphi'_1\tau' z = \varphi_{-1}\varphi''_1\theta_e z$$

et

$$\tau\varphi_{-1}\varphi'_1\theta_\nu\tau' z = \varphi_{-1}\varphi''_1\theta_\alpha z.$$

Voyons maintenant s'il pourra exister une fonction M des $n+2$ quantités $x_0, x_1, x_2,\ldots, x_{n-1}, x'_0, x''_0$, qui, considérée comme fonction des $n+1$ premières de ces quantités, soit semblable à $\Phi$ et soit invariable par les substitutions (B) et (C) et aussi par les substitutions (B′)

et (C′); de sorte que cette nouvelle fonction soit transitive une fois de plus que Φ.

Si la fonction M existe, les substitutions

$$
(\mathrm{B}'')\left\{
\begin{array}{l}
\left[\begin{array}{lll}
(x_z\,x_z), & (x_z\,x_{\theta_1 z}), & (x_z\,x_{\theta_{r-1} z}),\\
(x_z\,x_{\varphi'_1 z}), & (x_z\,x_{\varphi'_1\theta_1 z}), & (x_z\,x_{\varphi'_{n-1}\theta_{r-1} z}),
\end{array}\right]\\
\left[\begin{array}{lll}
(x_z\,x_{\varphi''_1 z}), & (x_z\,x_{\varphi''_1\theta_1 z}),\ldots, & (x_z\,x_{\varphi''_1\theta_{r-1} z}),\\
(x_z\,x_{\varphi''_1\varphi'_1 z}), & (x_z\,x_{\varphi''_1\varphi'_1\theta_1 z}),\ldots, & (x_z\,x_{\varphi''_1\varphi'_{n-1}\theta_{r-1} z}),
\end{array}\right]\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\left[\begin{array}{lll}
(x_z\,x_{\varphi''_{n-1} z}), & (x_z\,x_{\varphi''_{n-1}\theta_1 z}),\ldots, & (x_z\,x_{\varphi''_{n-1}\theta_{r-1} z}),\\
(x_z\,x_{\varphi''_{n-1}\varphi'_1 z}), & (x_z\,x_{\varphi''_{n-1}\varphi'_1\theta_1 z}),\ldots, & (x_z\,x_{\varphi''_{n-1}\varphi'_{n-1}\theta_{r-1} z}),
\end{array}\right]
\end{array}\right.
$$

$$
(\mathrm{C}'')\quad
\left[\begin{array}{lll}
(x_z\,x_{\varphi'_{-1}\varphi''_1 z}), & (x_z\,x_{\varphi'_{-1}\varphi''_1\theta_1 z}),\ldots, & (x_z\,x_{\varphi'_{-1}\varphi''_1\theta_{r-1} z}),\\
(x_z\,x_{\varphi'_{-1}\varphi''_1\varphi'_1 z}), & (x_z\,x_{\varphi'_{-1}\varphi''_1\varphi'_1\theta_1 z}),\ldots, & (x_z\,x_{\varphi'_{-1}\varphi''_1\varphi'_{n-1}\theta_{r-1} z}),
\end{array}\right]
$$

sont conjuguées entre elles; ce sont les seules qui effectuées sur $x_1$, $x_2, \ldots, x_{n-1}$, $x'_0$, $x''_0$, laissent invariable la fonction M, et l'on passe des substitutions (B), (C) aux substitutions (B″), (C″) par une même substitution.

Après cela, nous reconnaissons que cette fonction M est invariable par les $rn(n+1)(n+2)$ substitutions

$$
\begin{array}{ll}
(a) & (x_z\,x_{\varphi''_u\varphi'\varphi_t\theta_v z}),\\
(b) & (x_z\,x_{\varphi''_u\varphi_{-1}\varphi'_1\varphi_t\theta_v z}),\\
(c) & (x_z\,x_{\varphi_{-1}\varphi''_1\varphi'_s\varphi_t\theta_v z}),\\
(d) & (x_z\,x_{\varphi_{-1}\varphi''_1\varphi_{-1}\varphi'_1\varphi_t\theta_v z}),\\
(e) & (x_z\,x_{\varphi'_{-1}\varphi''_1\varphi'_s\varphi_t\theta_v z}),\\
(f) & (x_z\,x_{\varphi'_{-1}\varphi''_1\varphi_{-1}\varphi'_1\varphi_t\theta_v z}).
\end{array}
$$

Les substitutions $(e)$ et $(f)$ sont évidemment différentes entre elles, et elles sont évidemment différentes des substitutions $(a)$, $(b)$, $(c)$

$(d)$, puisque seules elles changent $x''_0$ en $x'_0$. Les substitutions $(c)$ et $(d)$ sont évidemment différentes entre elles, et elles sont différentes des substitutions $(a)$ et $(b)$, puisqu'elles changent $x''_0$ en $x_0$ et qu'aucune des substitutions $(a)$ et $(b)$ ne change $x''_0$ en $x_0$. Enfin les substitutions $(a)$ et $(b)$ sont évidemment différentes. Donc les substitutions $(a)$, $(b)$, $(c)$, $(d)$, $(e)$, $(f)$ étant toutes différentes, sont les seules qui laissent invariables la fonction M.

Actuellement je dis que, pour que la fonction M existe, il suffit que l'on puisse passer des substitutions (B), (C) aux substitutions (B''), (C'') par une même substitution.

Remarquons d'abord que les substitutions (B) et (C) peuvent être représentées par les deux expressions

$$\left(x_z\, x_{\varphi'_s \varphi_t \theta_\nu z}\right),\quad \left(x_z\, x_{\varphi_{-1} \varphi'_1 \varphi_t \theta_\nu z}\right);$$

elles sont pareillement données par les deux expressions

$$\left(x_z\, x_{\varphi_t \varphi'_s \theta_\nu z}\right),\quad \left(x_z\, x_{\varphi'_{-1} \varphi_1 \varphi'_t \theta_\nu z}\right).$$

Donc on a, quels que soient $s$ et $t$,

$$(g)\quad \left\{\begin{aligned} \varphi'_s \varphi_t \theta_\nu z &= \varphi_{t_1} \varphi'_{s_1} \theta_{\nu_1} z & \qquad \varphi_t \varphi'_s \theta_\nu z &= \varphi'_{s_1} \varphi_{t_1} \theta_{\nu_1} z \\ \text{ou } &= \varphi'_{-1} \varphi_1 \varphi'_{t_1} \theta_{\nu_1} z, & \text{ou } &= \varphi_{-1} \varphi'_1 \varphi_{t_1} \theta_{\nu_1} z. \end{aligned}\right.$$

Pareillement on a

$$(h)\quad \left\{\begin{aligned} \varphi''_s \varphi_t \theta_\nu z &= \varphi_{t_1} \varphi''_{s_1} \theta_{\nu_1} z & \qquad \varphi_t \varphi''_s \theta_\nu z &= \varphi''_{s_1} \varphi_{t_1} \theta_{\nu_1} z \\ \text{ou } &= \varphi''_{-1} \varphi_1 \varphi''_t \theta_u z, & \text{ou } &= \varphi_{-1} \varphi''_1 \varphi_{t_1} \theta_{\nu_1} z. \end{aligned}\right.$$

Enfin puisqu'on admet que l'on passe des substitutions (B), (C) aux substitutions (B''), (C'') par une même substitution, celles-ci sont conjuguées entre elles, et on a encore

$$(i)\quad \left\{\begin{aligned} \varphi''_s \varphi'_t \theta_\nu z &= \varphi'_{t_1} \varphi''_{s_1} \theta_{\nu_1} z & \qquad \varphi'_t \varphi''_s \theta_\nu z &= \varphi''_{s_1} \varphi_{t_1} \theta_{\nu_1} z \\ \text{ou } &= \varphi''_{-1} \varphi'_1 \varphi''_{t_1} \theta_{\nu_1} z, & \text{ou } &= \varphi'_{-1} \varphi''_1 \varphi'_{t_1} \theta_{\nu_1} z. \end{aligned}\right.$$

Observons enfin qu'on a les égalités :

$$(k) \qquad \theta_v \varphi_s z = \varphi_t \theta_u z, \quad \theta_v \varphi'_s z = \varphi'_t \theta_u z, \quad \theta_v \varphi''_s z = \varphi''_t \theta_v z.$$

Soient $\varphi^{(\alpha)}$ et $\varphi^{(\beta)}$ deux des fonctions $\varphi$, $\varphi'$, $\varphi''$ ; au lieu d'écrire les égalités $(g)$, $(h)$, $(i)$, nous pouvons dire qu'une fonction composée seulement des $\varphi^{(\alpha)}$, $\varphi^{(\beta)}$ et des $\theta$ peut s'écrire

$$\varphi^{(\alpha)}_u \varphi^{(\beta)}_s \theta_v z \quad \text{ou} \quad \varphi^{(\beta)}_{-1} \varphi^{(\alpha)}_1 \varphi^{(\beta)}_s \theta_v z.$$

Ceci établi, nous voyons aisément qu'en intervertissant l'ordre des fonctions $\varphi$, $\varphi'$, $\varphi''$, on pourra toujours ramener une substitution dérivée des substitutions (B), (C), (B'), (C') à une des formes $(a)$, $(b)$, $(c)$, $(d)$, $(e)$, $(f)$. Donc la fonction M existe.

*Remarque.* — S'il arrive que la substitution $(x_z\, x_{\chi z})$ ne fait que permuter les substitutions $(x_z\, x_{\varphi'' z})$, on passe des substitutions (B), (C) aux substitutions (B''), (C'') par la substitution $(x_z\, x_{\chi\tau z})$, et par conséquent la fonction M existe. En effet, on a dans ce cas

$$\chi\tau\varphi'_\alpha \varphi_\beta \theta_\gamma \tau' \chi' z = \chi\tau\varphi'_\alpha \tau' \chi' \chi\tau\varphi_\beta \theta_\gamma \tau' \chi' z = \chi\varphi''_\alpha \chi' \chi\varphi_v \theta_e \chi' z.$$

Or on a par hypothèse

$$\chi\varphi''_\alpha \chi' z = \varphi''_{\beta_1} z,$$

et on a d'ailleurs

$$\chi\varphi_v \theta_e \chi' z = \varphi'_s \theta_t z;$$

donc

$$\chi\tau\varphi'_\alpha \varphi_\beta \theta_\gamma \tau' \chi' z = \varphi''_{\beta_1} \varphi'_s \theta_t z.$$

*Application.* — Nous avons dit précédemment qu'il y a une fonction deux fois transitive de huit variables qui a 240 valeurs et qui est invariable par les substitutions

$$(m) \; (x_1 x_2 x_4)(x_3 x_6 x_5), \; (x_0 x_1 x_2 x_3 x_4 x_5 x_6), \; (x'_0 x_1 x_2 x_6 x_4 x_3 x_5),$$

ou par les substitutions

$$(m') \; (x_1 x_2 x_4)(x_3 x_6 x_5), \; (x_0 x_1 x_2 x_3 x_4 x_5 x_6) \; (x''_0 x_1 x_2 x_5 x_4 x_6 x_3).$$

et que l'on passe des substitutions $(m)$ aux substitutions $(m')$ par la substitution

$$(x_z x_{\tau z}) = (x_1 x_6)(x_2 x_5)(x_3 x_4).$$

La substitution $(x_z x_{\chi z})$ est ici $(x_3 x_6 x_5)$, et l'on passe des substitutions $(m)$ aux substitutions

$$(m'')\quad (x_6 x_5 x_2)(x_1 x_2 x_4), (x'_0 x_6 x_5 x_1 x_3 x_4 x_2), (x''_0 x_6 x_5 x_2 x_3 x_1 x_4)$$

par la substitution

$$(x_z x_{\tau\chi z}) = (x_1 x_6 x_2 x_5 x_4 x_3).$$

Donc il existe une fonction trois fois transitive de 9 quantités qui a 240 valeurs, invariable par les substitutions $(m)$ et $(m')$ (*).

Nous donnerons à la fin du chapitre suivant une application bien plus remarquable de cette théorie.

---

## CHAPITRE II.

### FONCTIONS DE $p^\nu$ QUANTITÉS INVARIABLES PAR DES SUBSTITUTIONS $(x_z x_{az p^\alpha + b})$ ET FONCTIONS DE $p^\nu + 1$ QUANTITÉS INVARIABLES PAR DES SUBSTITUTIONS $\left(x_z\, x_{\frac{A_{zp^\alpha} + B}{C_{zp^\alpha} + D}}\right)$.

Soit $p$ un nombre premier; en mettant comme indices à la lettre $x$ les $p^\nu$ quantités qui satisfont à la congruence $z^{p^\nu} \equiv z \pmod{p}$, nous avons étendu dans le *Journal* de M. Liouville (1860, p. 38), aux

---

(*) Cette fonction est donnée par ce théorème qui se trouve dans le Chapitre II : Si $p$ est un nombre premier, il y a une fonction trois fois transitive de $p^\nu + 1$ variables qui a $\dfrac{1.2.3\,..(p^\nu - 2)}{\nu}$ valeurs.

fonctions de $p^\nu$ et de $p^\nu + 1$ quantités des théorèmes que nous avions d'abord démontrés pour les fonctions de $p$ et de $p + 1$ variables; nous allons maintenant donner ici pour les premières fonctions des théorèmes qui leur sont propres, en adoptant les mêmes indices.

Soit $\tau$ un diviseur de $\nu$, et $u$ un diviseur de $p^\nu - 1$, il y a une fonction transitive de $p^\nu$ quantités invariable pour toutes les substitutions

$$(10) \qquad (z, \quad a^u z^{p^{\tau\alpha}} + b)$$

et qui a $\dfrac{1.2\ldots(p^\nu - 2)\times\tau}{\nu} \times u$ valeurs.

Soit $\psi$ une fonction invariable par la substitution $(z, z^{p^\tau})$, on formera une fonction invariable par toutes les substitutions (10) au moyen de $\psi$, comme on forme une fonction invariable par les substitutions $(z, a^u z + b)$ au moyen d'une fonction qui est changée par toute substitution.

Si nous supposons $u = 1$, nous aurons une fonction deux fois transitive de $p^\nu$ quantités invariable par les substitutions

$$(11) \qquad (z, az^{p^{\tau\alpha}} + b)$$

et qui a $\dfrac{1.2\ldots(p^\nu - 2)\times\tau}{\nu}$ valeurs.

Soit $\tau$ un diviseur de $\nu$, il existe une fonction trois fois transitive de $p^\nu + 1$ quantités qui a $\dfrac{1.2\ldots(p^\nu - 2)\times\tau}{\nu}$ valeurs, et qui est invariable par toutes les substitutions

$$(12) \qquad \left(z, \frac{Az^{p^{\tau\alpha}} + B}{Cz^{p^{\tau\alpha}} + D}\right).$$

Soit F une fonction deux fois transitive invariable par toutes les substitutions (11); on construira une fonction invariable par toutes les substitutions (12) au moyen de F, de la même manière que l'on forme une fonction invariable par toutes les substitutions $\left(z, \dfrac{Az + B}{Cz + D}\right)$ au moyen d'une fonction invariable par les substitutions $(z, az + b)$.

Soit $\tau$ un diviseur de $\nu$, et $p$ différent de 2, il existe une fonction $\Lambda$ deux fois transitive de $p^\nu + 1$ variables qui a $\frac{1.2\ldots(p^\nu - 2)}{\nu} \times 2\tau$ valeurs, et qui est invariable par les substitutions (12) pour lesquelles AD — BC est un résidu quadratique.

Nous formerons la fonction $\Lambda$ au moyen de la fonction $\lambda$ invariable par les substitutions $(z, a^2 z^{p^{\tau\alpha}} + b)$ de la même manière que l'on peut former la fonction invariable par les substitutions $\left(z, \frac{Az + B}{Cz + D}\right)$ pour lesquelles AD — BC est résidu quadratique au moyen de la fonction invariable par les substitutions $(z, a^2 z + b)$. Ainsi faisons sur $\lambda$ toutes les substitutions $\left(\frac{1}{z}, \frac{1}{z+n}\right)$, nous obtiendrons ainsi les $p^\nu - 1$ fonctions $\lambda_1, \lambda_2, \ldots, \lambda_{p^\nu - 1}$; faisons encore sur $\lambda$ la substitution $\left(z, \frac{(-1)^{\frac{p^\nu - 1}{2}}}{z}\right)$ ce qui donnera $\lambda'$; enfin formons une fonction symétrique de $\lambda, \lambda_1, \ldots, \lambda_{p^\nu - 1}, \lambda'$, et nous aurons $\Lambda$.

La substitution $(z, z^{p^\tau})$ peut changer ou laisser invariable la fonction qui a deux valeurs; dans le premier cas, en multipliant $\Lambda$ par la fonction qui a deux valeurs, on obtient une fonction qui a un nombre de valeurs double; dans le second cas, on obtient une autre fonction semblable à $\Lambda$.

Supposons $\nu$ pair et $p$ différent de 2, et soit $2\tau$ un diviseur de $\nu$; il existe une fonction deux fois transitive de $p^\nu$ quantités qui a $\frac{1.2\ldots(p^\nu - 2)}{\nu} \times 2\tau$ valeurs, et qui est invariable par toutes les substitutions renfermées dans les deux expressions

$$(13)\qquad \left(z, \omega^{2r} z^{p^{2\alpha\tau}} + m\right), \quad \left(z, \omega^{2s+1} z^{p^{(2\alpha+1)\tau}} + n\right),$$

$\omega$ étant une racine primitive de $z^{p^\nu - 1} \equiv 1 \pmod{p}$.

Pour construire cette fonction deux fois transitive, nous formerons une fonction $\varphi$ invariable par les substitutions

$$\left(z, \omega^{2r} z^{p^{2\alpha\tau}}\right), \quad \left(z, \omega^{2s+1} z^{p^{(2\alpha+1)\tau}}\right);$$

nous ferons sur cette fonction toutes les substitutions $(z, z+m)$, nous obtiendrons les fonctions $\varphi, \varphi_1, \varphi_2, \ldots, \varphi_{p^\nu-1}$ et nous prendrons une fonction symétrique $\Psi$ de ces $p^\nu$ fonctions.

On voit encore que, $u$ étant un diviseur impair de $p^\nu - 1$, il y a une fonction transitive de $p^\nu$ quantités qui a $\frac{1.2\ldots(p^\nu-2)}{\nu} \times 2\tau \times u$ valeurs, et qui est invariable par les substitutions (13), dans lesquelles $\omega$ est remplacé par $\omega^u$.

Supposons $\nu$ pair, $p$ différent de 2, et $2\tau$ un diviseur de $\nu$; il existe une fonction trois fois transitive de $p^\nu + 1$ quantités, qui a $\frac{1.2\ldots(p^\nu-2)}{\nu} \times 2\tau$ valeurs, et qui est invariable par les substitutions

$$(14)\qquad \left(z, \frac{A z^{p^{2\alpha\tau}} + B}{C z^{p^{2\alpha\tau}} + D}\right), \quad \left(z, \frac{A_1 z^{p^{(2\alpha+1)\tau}} + B_1}{C_1 z^{p^{(2\alpha+1)\tau}} + D_1}\right),$$

$AD - BC$ étant résidu quadratique, et $A_1 D_1 - B_1 C_1$ non résidu.

On construit cette fonction trois fois transitive au moyen de la fonction $\Psi$ invariable par les substitutions (13) de la même manière que l'on forme la fonction invariable par les substitutions $\left(z, \frac{Az+B}{Cz+D}\right)$, pour lesquelles $AB - BC$ est résidu quadratique au moyen de la fonction invariable par les substitutions $(z, a^2 z + b)$.

*Remarque.* — Ces différents théorèmes donnent des fonctions qui ont le même nombre de valeurs, sans être semblables. Ainsi dans le cas où $\frac{\nu}{\tau}$ est pair, il y a deux fonctions trois fois transitives et une fonction deux fois transitive de $p^\nu + 1$ quantités qui ont $\frac{1.2\ldots(p^\nu-2) \times 2\tau}{\nu}$ valeurs. L'une de ces fonctions trois fois transitive est celle qui n'est pas changée par les substitutions (14); l'autre fonction trois fois transitive est celle qui est invariable par toutes les substitutions

$$\left(z, \frac{A z^{p^{2\alpha\tau}} + B}{C z^{p^{2\alpha\tau}} + D}\right);$$

enfin la fonction deux fois transitive est celle qui est invariable par toutes les substitutions

$$\left(z, \frac{Az^{p^{\alpha\tau}}+B}{Cz^{p^{\alpha\tau}}+D}\right),$$

pour lesquelles AD — BC est résidu quadratique.

*Étude des substitutions* $\left(z, \frac{Az^{p^{\alpha}}+B}{Cz^{p^{\alpha}}+D}\right)$.

Parmi ces substitutions considérons d'abord la substitution $(z, z^p)$ et ses puissances $\left(z, z^{p^\alpha}\right)$.

Les racines de la congruence $z^p \equiv z \pmod{p}$ sont $0, 1, 2, \ldots, p-1$; donc la substitution $(z, z^p)$ laisse immobiles les variables $x_0, x_1, x_2, \ldots, x_{p-1}$ et permute les $p^\nu - p$ autres variables.

Si $\nu$ est un nombre premier, la substitution $(z, z^p)$ est une substitution régulière composée de $\frac{p^\nu - p}{\nu}$ cycles de $\nu$ quantités. Car $x_k, x_{kp}, x_{kp^2}, \ldots, x_{kp^{\nu-1}}$ sont des variables différentes. La substitution $\left(z, z^{p^r}\right)$ est semblable à $(z, z^p)$.

Si $\nu$ est un nombre composé, les racines de $z^{p^\alpha} \equiv z$ qui appartiennent à $z^{p^\nu} \equiv z$ sont celles de la congruence $z^{p^\tau} \equiv z$, $\tau$ étant le plus grand commun diviseur de $\nu$ et de $\alpha$; par conséquent la substitution $\left(z, z^{p^\alpha}\right)$ s'effectue alors seulement sur $p^\nu - p^\tau$ variables.

Considérons en second lieu les substitutions

$$(a) \qquad \left(z, az^{p^\alpha}\right)$$

et soit $\tau$ le plus grand commun diviseur de $\alpha$ et de $\nu$. D'après ce qui a été dit au commencement du chapitre I, il résulte du mode même de formation des fonctions qui sont invariables par les substitutions $(a)$, que les substitutions qui ont moins de $p^\nu - 1$ variables sont de la

forme $\left(kz, kz^{p^\alpha}\right)$ ou de la forme

$$(b) \qquad \left(z, l^{p^\alpha - 1} z^{p^\alpha}\right);$$

ce sont donc les substitutions $(a)$ pour lesquelles $a$ est résidu de puissance $(p^\nu - 1)^{ième}$; par conséquent aussi les substitutions $(a)$ pour lesquelles $a$ n'est pas résidu de puissance $(p^\nu - 1)^{ième}$ s'effectuent sur $p^\nu - 1$ quantités.

Occupons-nous ensuite des substitutions

$$(c) \qquad \left(z, az^{p^\alpha} + b\right).$$

Reportons-nous à la manière de former une fonction invariable par les substitutions $(c)$ au moyen d'une fonction invariable par les substitutions $(a)$, et nous reconnaissons que toutes les substitutions $(c)$ qui ont moins de $p^\nu$ variables sont de la forme

$$(d) \qquad \left(z + m, az^{p^\alpha} + m\right),$$

et sont semblables aux substitutions $(a)$; les substitutions $(d)$ peuvent encore s'écrire

$$\left(z, az^{p^\alpha} - am^{p^\alpha} + m\right).$$

D'après cela, pour que la substitution $(c)$ s'effectue sur moins de $p^\nu$ quantités, il faut que l'on puisse trouver une valeur de $m$ satisfaisant à la congruence

$$-am^{p^\alpha} + m \equiv b$$

ou

$$am^{p^\alpha} - m + b \equiv 0;$$

si au contraire $b$ est tel qu'il n'y ait aucun diviseur commun au premier membre de cette congruence et à $m^{p^\nu - 1} - 1$, la substitution $(c)$ s'effectue sur $p^\nu$ variables.

Nous avons examiné ces différents cas particuliers de la substitution

$$(e)\qquad \left(z,\ \frac{Az^{p^\alpha}+B}{Cz^{p^\alpha}+D}\right),$$

parce que toutes les substitutions $(e)$ qui s'effectuent sur moins de $p^\nu+1$ variables sont semblables aux substitutions que nous venons de considérer; nous allons maintenant passer au cas général.

Pour étudier les substitutions $(e)$, nous allons procéder comme nous l'avons fait pour les substitutions $\left(z,\ \frac{Az+B}{Cz+D}\right)$. (*Journal de M. Liouville*, année 1860.)

$\omega$ étant une racine primitive de $z^{p^\nu-1}\equiv 1$, soit

$$(f)\qquad \varphi\left[(x_0),\ x_1,\ x_\omega,\ x_{\omega^2},\ldots,\ x_{\omega^{p^\nu-2}}\right]$$

une fonction qui est invariable par toutes les substitutions $\left(z,\ az^{p^\alpha}\right)$; faisons sur cette fonction toutes les substitutions $(z,\ z+m)$ et formons une fonction symétrique F de ces $p^\nu$ fonctions; sur la fonction F faisons la substitution $\left(z,\ \frac{1}{z}\right)$, nous aurons la fonction F′; enfin sur la fonction F′ faisons les substitutions $\left(\frac{1}{z},\ \frac{1}{z+k}\right)$, ce qui donnera les fonctions $F'$, $F'_1,\ldots,$ $F'_{p^\nu-1}$; soit $\Theta$ une fonction symétrique des $p^\nu+1$ fonctions F, $F'$, $F'_1,\ldots,$ $F'_{p^\nu-1}$; $\Theta$ est une fonction invariable par les substitutions $(e)$, et les substitutions qui ne changent pas ces fonctions F sont les substitutions $(e)$ qui s'effectuent sur moins de $p^\nu+1$ quantités.

La fonction $F'_u$ contient la fonction

$$\varphi\left[\left(x_{\frac{1}{r}+u}\right),\ x_{\frac{1}{r+1}+u},\ x_{\frac{1}{r+\omega}+u},\ x_{\frac{1}{r+\omega^2}+u},\ldots,\ x_{\frac{1}{r+\omega^{p^\nu-2}}+u}\right],$$

qui est invariable par les substitutions

$$(g)\qquad \left(\frac{1}{r+z}+u,\quad \frac{1}{r+az^{p^\alpha}}+u\right),$$

puisque la fonction $(f)$ est invariable par les substitutions $\left(z, az^{p^\alpha}\right)$: donc $F'_u$ est aussi invariable par les substitutions $(g)$.

On met facilement les substitutions $(g)$ sous cette forme

$$(h) \qquad \left| z, \frac{\left(\frac{1}{r - ar^{p^\alpha}} + u\right) z^{p^\alpha} - u^{p^\alpha + 1} + \frac{au - u^{p^\alpha}}{r - ar^{p^\alpha}}}{z^{p^\alpha} + \frac{a}{r - ar^{p^\alpha}} - u^{p^\alpha}} \right|.$$

En donnant à $r$ et $u$ les $p^\nu$ valeurs dont ils sont susceptibles, on aura toutes les substitutions qui ont moins de $p^\nu + 1$ variables, et qui ne changent pas les fonctions $F'$, $F'_1$, $F'_2, \ldots$, $F'_{p^\nu - 1}$; il n'y a pas lieu d'ajouter aux substitutions $(h)$ les substitutions $\left(z, mz^{p^\alpha} + n\right)$ qui laissent F invariable; car ces dernières substitutions se déduisent de l'expression $(h)$ en y faisant

$$r \equiv 0.$$

Les substitutions $(h)$ ou $(g)$ qui s'effectuent sur moins de $p^\nu - 1$ variables sont celles pour lesquelles $a$ est résidu de puissance $(p^\tau - 1)^{ième}$, $\tau$ étant le plus grand commun diviseur de $\alpha$ et de $\nu$.

Les deux variables $x_u$ et $x_{\frac{1}{r} + u}$ sont laissées immobiles par les substitutions $(h)$; si cette substitution s'effectue sur moins de $p^\nu - 1$ quantités, les autres quantités qui resteront immobiles seront celles dont les indices sont racines de la congruence $z^{p^\alpha - 1} \equiv \frac{1}{a}$.

La puissance $s^{ième}$ de la substitution $(g)$ ou $(h)$ s'obtient en y changeant $a$ en $a^{\frac{p^{s\alpha} - 1}{p - 1}}$ et $z^{p^\alpha}$ en $z^{p^{\alpha s}}$.

Les substitutions de $p^\nu$ quantités qui laissent F invariable sont les substitutions $\left(z, az^{p^\alpha} + n\right)$, dans lesquelles $n$ est tel que $am^{p^\alpha} - m + n$ n'a aucun diviseur commun avec $m^{p^\nu - 1} - 1$; $n$ étant pris de la même manière, toutes les substitutions de $p^\nu$ variables qui ne changent pas $F'_u$

sont données par l'expression

$$(k)\qquad \left(z,\ \frac{\left(\frac{1}{n}+u\right)z^{p^\alpha}-u^{p^\alpha+1}+\frac{au-u^{p^\alpha}}{n}}{z^{p^\alpha}+\frac{a}{n}-u^{p^\alpha}}\right);$$

nous avons donc toutes les substitutions $(e)$ qui s'effectuent sur $p^\nu$ quantités.

On voit d'après cela que, excepté la substitution $\left(z,\ az^{p^\alpha}+n\right)$ de $p^\nu$ variables, toutes les substitutions $(e)$ qui s'effectuent sur moins de $p^\nu+1$ quantités sont représentées par l'expression $(k)$, $n$ étant alors quelconque.

Si la substitution $(e)$ s'effectue sur les $p^\nu+1$ quantités, elle peut encore être représentée par l'expression $(k)$, mais à la condition que $a, u, n$ ne soient plus de la forme $\alpha_0+\alpha_1 i+\ldots+\alpha_{\nu-1}i^{\nu-1}$, $\alpha_0, \alpha_1$, etc., étant entiers et $i$ racine d'une congruence irréductible du degré $\nu$; il faudra d'ailleurs que l'on ait

$$(m)\qquad \frac{1}{n}+u\equiv\frac{A}{C},\quad -u^{p^\alpha+1}+\frac{au-u^{p^\alpha}}{n}\equiv\frac{B}{C},\quad \frac{a}{n}-u^{p^\alpha}\equiv\frac{D}{C},$$

A, B, C, D étant de la forme $\alpha_0+\alpha_1 i+\ldots+\alpha_{\nu-1}i^{\nu-1}$.

Des congruences $(m)$ on tire les deux suivantes :

$$\frac{A^{p^\alpha}+DC^{p^\alpha-1}}{C^{p^\alpha}}\equiv\frac{1+an^{p^\alpha-1}}{n^{p^\alpha}},\quad \frac{AD-BC}{C^2}\equiv\frac{a}{n^2},$$

et en les joignant à la première congruence $(m)$, on en tirera facilement ces trois autres équations qui donnent $n$, $a$ et $u$ :

$$(q)\qquad \frac{AD-BC}{C^2}n^{p^\alpha+1}-\frac{A^{p^\alpha}+DC^{p^\alpha-1}}{C^{p^\alpha}}n^{p^\alpha}+1\equiv 0,$$

$$a\equiv n^2\frac{AD-BC}{C^2},\quad u\equiv\frac{1}{n}-\frac{A}{C}.$$

Donc s'il y a une valeur de $u$ de la forme $\alpha_0 + \alpha_1 i + \ldots + \alpha_{\nu-1} i^{\nu-1}$ satisfaisant à $(q)$, les valeurs de $a$ et de $u$ sont de la même forme; donc aussi, pour que la substitution $(e)$ s'effectue sur $p^\nu + 1$ quantités, la condition nécessaire et suffisante est que le premier membre de la congruence $(q)$ n'ait aucun diviseur commun avec $n^{p^\nu-1} - 1$.

D'après cela, supposons que $\lambda$ et $\mu$ soient pris de telle sorte que la congruence

$$n^{p^\alpha+1} - \lambda n^{p^\alpha} + \mu \equiv 0$$

soit irréductible, c'est-à-dire que son premier membre n'ait aucun facteur commun avec $n^{p^\nu-1} - 1$. Posons

$$\frac{A^{p^\alpha} + DC^{p^\alpha-1}}{C^{p^\alpha-2}(AD - BC)} \equiv \lambda, \quad \frac{C^2}{AD - BC} \equiv \mu;$$

nous en tirerons

$$\frac{D}{C} \equiv \frac{\lambda}{\mu} - \frac{A^{p^\alpha}}{C^{p^\alpha}}, \quad \frac{B}{C} \equiv \frac{A\lambda}{C\mu} - \frac{A^{p^\alpha+1}}{C^{p^\alpha+1}} - \frac{1}{\mu}.$$

On voit d'après cela que pour chaque système de valeurs de $\lambda$ et de $\mu$, nous aurons $p^\nu$ systèmes de valeurs pour $\frac{A}{C}, \frac{B}{C}, \frac{D}{C}$, et les substitutions de $p^\nu + 1$ variables peuvent s'écrire

$$\left(z, \frac{A}{C} - \frac{1}{\mu z^{p^\alpha} + \lambda - \mu \frac{A^{p^\alpha}}{C^{p^\alpha}}}\right).$$

*Fonction cinq fois transitive de douze quantités ayant*
$1.2.3.4.5.6.7 = 5040$ *valeurs.*

En nous appuyant sur ce qui a été dit dans ce chapitre et surtout sur ce qui a été exposé à la fin du chapitre I<sup>er</sup>, nous pouvons facilement

démontrer l'existence d'une fonction cinq fois transitive de douze quantités.

Soit $\omega$ une racine de la congruence irréductible

$$\omega^2 + 2\omega + 2 \equiv 0 \pmod{3},$$

et considérons la fonction deux fois transitive des neuf quantités $x_0$, $x_1$, $x_2$, $x_\omega$, $x_{1+\omega}$, $x_{2+\omega}$, $x_{2\omega}$, $x_{1+2\omega}$, $x_{2+2\omega}$, qui est invariable par toutes les substitutions comprises dans les deux expressions

$$(l) \qquad (x_z\, x_{\omega^{2r}z+m}), \quad (x_z\, x_{\omega^{2r+1}z^3+m});$$

celles de ces substitutions qui ne s'effectueront que sur $x_1$, $x_2$, $x_\omega$, $x_{1+\omega}$, $x_{2\omega}$, $x_{1+2\omega}$, $x_{2+\omega}$, $x_{2+2\omega}$, sont les suivantes :

$$(m) \qquad (x_z\, x_{\omega^2 z}) = (x_1\, x_{1+\omega}\, x_2\, x_{2+2\omega})(x_\omega\, x_{1+2\omega}\, x_{2\omega}\, x_{2+\omega}),$$

$$(n) \qquad (x_z\, x_{\omega^3 z^3}) = (x_1\, x_{1+2\omega}\, x_2\, x_{2+\omega})(x_{2+2\omega}\, x_{2\omega}\, x_{1+\omega}\, x_\omega),$$

$$(p) \qquad (x_z\, x_{\omega^5 z^3}) = (x_1\, x_{2\omega}\, x_2\, x_\omega)(x_{2+\omega}\, x_{1+\omega}\, x_{1+2\omega}\, x_{2+2\omega}),$$

$$(x_z\, x_{\omega^4 z}) = (x_1\, x_2)(x_{1+\omega}\, x_{2+2\omega})(x_\omega\, x_{2\omega})(x_{1+2\omega}\, x_{2+\omega}),$$

et leurs inverses; de plus toutes les substitutions $(l)$ sont des dérivées de celles-là et de

$$(q) \qquad (x_0\, x_1\, x_2)(x_\omega\, x_{1+\omega}\, x_{2+\omega})(x_{2\omega}\, x_{1+2\omega}\, x_{2+2\omega}).$$

Identifions la substitution

$$(x_1\, x_{1+\omega}\, x_2\, x_{2+2\omega})(x_\omega\, x_{1+2\omega}\, x_{2\omega}\, x_{2+\omega})$$

avec

$$(x'_1\, x'_{2+2\omega}\, x'_2\, x'_{1+\omega})(x'_{2+\omega}\, x'_{2\omega}\, x'_{1+2\omega}\, x'_\omega);$$

nous pouvons faire $x'_1 = x_1$, et nous avons pour les quatre identifications :

$$x'_1 = x_1, \quad x'_{2+2\omega} = x_{1+\omega}, \quad x'_2 = x_2, \quad x'_{1+\omega} = x_{2+2\omega},$$

avec

$$1^\circ \quad x'_{2+\omega} = x_\omega, \quad x'_{2\omega} = x_{1+2\omega}, x'_{1+2\omega} = x_{2\omega}, \quad x'_\omega = x_{2+\omega};$$

$$2^\circ \quad x'_{2\omega} = x_\omega, x'_{1+2\omega} = x_{1+2\omega}, \quad x'_\omega = x_{2\omega}, x'_{2+\omega} = x^{2+\omega};$$

$$3^\circ \quad x'_{1+2\omega} = x_\omega, \quad x'_\omega = x_{1+2\omega}, \quad x'_{2+\omega} = x_{2\omega}, \quad x'_{2\omega} = x_{2+\omega};$$

$$4^\circ \quad x'_\omega = x_\omega, \quad x'_{2+\omega} = x_{1+2\omega}, \quad x'_{2\omega} = x_{2\omega}, \quad x'_\omega = x_{2+\omega}.$$

Pour chacune de ces identifications la substitution

$$(x'_0\, x'_1\, x'_2)(x'_\omega\, x'_{1+\omega}\, x'_{2+\omega})(x'_{2\omega}\, x'_{1+2\omega}\, x'_{2+2\omega})$$

devient respectivement

$$1^\circ \qquad (x'_1\, x_1\, x_2)(x_{2+\omega}\, x_{2+2\omega}\, x_\omega)(x_{1+2\omega}\, x_{2\omega}\, x_{1+\omega}),$$

$$2^\circ \qquad (x'_0\, x_1\, x_2)(x_{2\omega}\, x_{2+2\omega}\, x_{2+\omega})(x_\omega\, x_{1+2\omega}\, x_{1+\omega}),$$

$$3^\circ \qquad (x'_0\, x_1\, x_2)(x_{1+2\omega}\, x_{2+2\omega}\, x_{2\omega})(x_{2+\omega}\, x_\omega\, x_{1+\omega}),$$

$$4^\circ \qquad (x'_0\, x_1\, x_2)(x_\omega\, x_{2+2\omega}\, x_{1+2\omega})(x_{2\omega}\, x_{2+\omega}\, x_{1+\omega}).$$

En cherchant quelques dérivées de la substitution 3° et des substitutions $(m)$, $(n)$, $(q)$, on reconnaît immédiatement que la substitution 3° ne saurait donner une fonction trois fois transitive de dix variables.

Prenons les substitutions $(m)$, $(n)$, $(p)$, $(q)$ avec la substitution 1°, nous aurons un système que nous appellerons A; prenons les substitutions $(m)$, $(n)$, $(p)$, $(q)$, avec la substitution 2°, nous aurons un système B; enfin, prenons encore $(m)$, $(n)$, $(p)$, $(q)$ avec 4°, nous aurons le système C.

On voit facilement que pour la première identification on a $x'_z = x_{\chi z} = x_{\frac{1}{z}}$, et par suite qu'il existe une fonction invariable par le système A, et qu'elle est invariable par toutes les substitutions comprises dans les deux expressions

$$\left(x_z\, x_{\frac{Az+B}{Cz+D}}\right), \quad \left(x_z\, x_{\frac{A_1 z^3+B_1}{C_1 z^3+D_1}}\right),$$

AD — BC étant résidu quadratique et $A_1 D_1 - B_1 C_1$ non résidu.

On reconnaît ensuite que l'on passe du système A au système B par la substitution

$$(x_{1+\omega} x_{1+2\omega})(x_{\omega} x_{2\omega})(x_{2+2\omega} x_{2+\omega});$$

on passe aussi du système A au système C par la substitution

$$(x_{1+\omega} x_{2\omega})(x_{2+2\omega} x_{\omega})(x_{1+2\omega} x_{2+\omega}).$$

Pour la première identification on a $x'_z = x_{\chi z} = x_{\frac{1}{z}}$, et la substitution $(x_z x_{\chi z}) = \left(x_z x_{\frac{1}{z}}\right)$ ne change pas les substitutions 2° et 4°.

Il résulte donc de la théorie exposée à la fin du chapitre I et en particulier de la dernière remarque que nous y avons faite, que l'on passe par une même substitution du système dérivé de

$$(m), (n), (p), (q), \quad 1^\circ,$$

non-seulement au système dérivé de

$$(m), (n), (p), (q), \quad 2^\circ,$$

mais encore au système dérivé de

$$(m), (n), (p), (q), \quad 3^\circ.$$

Et pareillement on passe par une même substitution du système des substitutions dérivées de

$$(m), (n), (p), (q) \quad 1^\circ$$

au système des substitutions dérivées de

$$(m), (n), (p), (q), \quad 4^\circ$$

et au systeme des substitutions dérivées de

$$(m), (n), (p), \quad 1^\circ \text{ et } 4^\circ.$$

Nous avons donc bien une fonction cinq fois transitive des douze variables $x_1$, $x_2$, $x_\omega$, $x_{1+\omega}$, $x_{2\omega}$, $x_{1+2\omega}$, $x_{2+\omega}$, $x_{2+2\omega}$, $x_0$, $x'_0$, $x''_0$, $x'''_0$, et on caractérise cette fonction en disant qu'elle est invariable par les substitutions $(l)$ et par les substitutions

$$(x'_0\, x_1\, x_2)(x_{2+\omega}\, x_{2+2\omega}\, x_\omega)(x_{1+2\omega}\, x_{2\omega}\, x_{1+\omega}),$$
$$(x''_0\, x_1\, x_2)(x_{2\omega}\, x_{2+2\omega}\, x_{2+\omega})(x_\omega\, x_{1+2\omega}\, x_{\omega+1}),$$
$$(x'''_0\, x_1\, x_2)(x_\omega\, x_{2+2\omega}\, x_{1+2\omega})(x_{2\omega}\, x_{2+\omega}\, x_{1+\omega}).$$

Enfin j'énoncerai encore sur cette fonction la remarque suivante que je ne démontrerai pas : Si on remplace les variables

$$x''_0,\ x'_0,\ x_\omega,\ x_{1+\omega},\ x_{2+2\omega},\ x_{1+2\omega},\ x_2,\ x_1,\ x_0,\ x_{2+\omega},\ x_{2\omega},\ x'''_0$$

par

$$x_0,\ x_1,\ x_2,\ x_3,\ x_4,\ x_5,\ x_6,\ x_7,\ x_8,\ x_9,\ x_{10},\ x_\infty,$$

respectivement, cette fonction de douze quantités est invariable par toutes les substitutions

$$\left(z,\ \frac{Az+B}{Cz+D}\right) \pmod{11}.$$

AD — BC étant résidu quadratique.

Je possède une fonction cinq fois transitive de 24 quantités qui a $\dfrac{1.2.3.4\ldots18.19}{16\times3}$ valeurs, et qui est due à des circonstances différentes de celles qui donnent la fonction cinq fois transitive de douze quantités dont nous venons de parler [*].

[*] En joignant cette fonction cinq fois transitive aux fonctions de moins de trente-quatre quantités qui sont données par nos théorèmes généraux, on voit que l'on a des fonctions plusieurs fois transitives de $n$ quantités, tant que $n$ est $< 34$; ce fait tient simplement à ce que tous les nombres $< 34$, excepté 21 et 22, sont des nombres premiers, des puissances de nombres premiers, ou de tels nombres augmentés d'une unité, ou enfin des puissances de 2 diminuées d'une unité.

## CHAPITRE III.

### FONCTIONS PLUSIEURS FOIS TRANSITIVES DE $p^\nu$ VARIABLES ($p$ NOMBRE PREMIER), QUI ONT $\dfrac{1.2.3\ldots(p^\nu-1)}{(p^\nu-1)(p^\nu-p)\ldots(p^\nu-p^{\nu-1})}$ VALEURS

*De la formation de ces fonctions.*

Considérons un système de $p^\nu$ variables, et comme dans le chapitre précédent désignons-les par la lettre $x$ affectée de $p^\nu$ indices qui soient les racines de la congruence

$$(1)\qquad z^{p^\nu}-z\equiv 0 \pmod{p};$$

nous allons maintenant nous occuper des fonctions de ces $p^\nu$ variables qui ne sont pas changées par toutes les substitutions

$$(2)\qquad (z,\ Az^{p^{\nu-1}}+Bz^{p^{\nu-2}}+Cz^{p^{\nu-3}}+\ldots+Hz+L).$$

Il faut immédiatement remarquer que dans l'expression (2), A, B, C,..., L ne sont pas des racines de la congruence (1) prises arbitrairement; pour que l'expression (2) représente une substitution, il faut en effet que le polynôme $Az^{p^{\nu-1}}+Bz^{p^{\nu-2}}+\ldots+Hz$ n'ait aucun facteur commun avec $z^{p^\nu}-z$, afin que, $z_1$ et $z_2$ étant deux racines de la congruence (1), on ne puisse avoir

$$Az_1^{p^{\nu-1}}+Bz_1^{p^{\nu-2}}+\ldots+Hz_1\equiv Az_2^{p^{\nu-1}}+Bz_2^{p^{\nu-2}}+\ldots+Hz_2$$

ou

$$A(z_1-z_2)^{p^{\nu-1}}+B(z_1-z_2)^{p^{\nu-2}}+\ldots+H(z_1-z_2)\equiv 0.$$

Cela posé, on a identiquement

$$(3)\quad\begin{cases} h(z^{p^\nu}-z)\equiv\left(h^{p^{\nu-1}}z^{p^{\nu-1}}+h^{p^{\nu-2}}z^{p^{\nu-2}}+\ldots+h^pz^p+hz\right)\\ \times\left(h^{p^{\nu-1}}z^{p^{\nu-1}}+\ldots+hz+1\right)\left(h^{p^{\nu-1}}z^{p^{\nu-1}}+\ldots+hz+2\right)\cdots\\ \times\left(h^{p^{\nu-1}}z^{p^{\nu-1}}+\ldots+hz+p-1\right).\end{cases}$$

Soient $\alpha^{1,1}$, $\alpha^{1,2}$, $\alpha^{1,3}, \ldots, \alpha^{1,p^\nu-1}$ les racines de $z^{p^\nu} \equiv z$ dues au premier facteur, $\alpha^{2,1}$, $\alpha^{2,2}, \ldots, \alpha^{2,p^\nu-1}$ les racines dues au second, $\alpha^{3,1}$, $\alpha^{3,2}, \ldots, \alpha^{3,p^\nu-1}$ celles qui sont dues au troisième, et ainsi de suite. Prenons la fonction

$$(4)\quad \left\{\begin{aligned} & x_{\alpha^{1,1}} x_{\alpha^{1,2}} x_{\alpha^{1,3}} \ldots x_{\alpha^{1,p^\nu-1}} + x_{\alpha^{2,1}} x_{\alpha^{2,2}} \ldots x_{\alpha^{2,p^\nu-1}} + \ldots \\ & \qquad + x_{\alpha^{p,1}} x_{\alpha^{p,2}} \ldots x_{\alpha^{p,p^\nu-1}}; \end{aligned}\right.$$

nous pouvons donner à $h$ dans l'expression (3) $p^\nu - 1$ valeurs; mais si $e$ est une racine de $z^{p-1} \equiv 1$, $h = h_1$ et $h = h_1 e$ donnent les mêmes facteurs; de sorte que pour décomposer $z^{p^\nu} - z$ de toutes les manières possibles en facteurs comme dans l'identité (3), il suffit de donner à $h$ $\frac{p^\nu - 1}{p-1}$ valeurs; à chaque décomposition de $z^{p^\nu} - z$ correspond une fonction telle que (4); prenons une fonction symétrique $\Phi$ de ces $\frac{p^\nu - 1}{p-1}$ fonctions, et nous aurons une fonction qui est invariable par toutes les substitutions (2). Il est clair d'après cela que l'on obtiendra la fonction $\Phi$ en faisant sur la fonction (4) les substitutions

$$(z, z), \quad (z, \omega z), \quad (z, \omega^2 z), \ldots, \quad \left(z, \omega^{\frac{p^\nu - p}{p-1}} z\right),$$

$\omega$ étant une racine primitive de $z^{p^\nu-1} \equiv 1$, et en formant une fonction symétrique des $\frac{p^\nu - 1}{p-1}$ fonctions ainsi obtenues.

Pour démontrer que la fonction $\Phi$ est invariable par toutes les substitutions (2), il suffit évidemment de prouver qu'une telle substitution change les indices qui satisfont à l'une des congruences

$$(5)\quad \left\{\begin{aligned} & h^{p^\nu-1} z^{p^\nu-1} + h^{p^\nu-2} z^{p^\nu-2} + \ldots + h^p z^p + hz \equiv 0, \\ & \qquad h^{p^\nu-1} z^{p^\nu-1} + \ldots + hz + 1 \equiv 0, \ldots, \\ & \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & \qquad h^{p^\nu-1} z^{p^\nu-1} + \ldots + hz + p - 1 \equiv 0, \end{aligned}\right.$$

en les indices qui satisfont à l'une de celles-ci :

$$(6)\quad \left\{\begin{array}{l} h'^{p^{\nu-1}} z^{p^{\nu-1}} + h'^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h'^{p} z^{p} + h' z \equiv 0, \\ h'^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h' z + 1 \equiv 0, \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ h'^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h' z + p - 1 \equiv 0. \end{array}\right.$$

Par la substitution (2) la racine $z$ d'une des congruences (5) sera changée en

$$u \equiv A z^{p^{\nu-1}} + B z^{p^{\nu-2}} + \ldots + H z + L,$$

et de cette congruence on tirera

$$(7)\quad z \equiv a u^{p^{\nu-1}} + b u^{p^{\nu-2}} + \ldots + l u^{p} + m u + n,$$

en désignant par

$$\left(z,\ a z^{p^{\nu-1}} + b z^{p^{\nu-2}} + \ldots + m u + n\right)$$

la substitution inverse de la substitution (2). Si donc nous remplaçons $z$ par l'expression (7) dans les congruences (5), chacune des congruences qui en résulteront, donnera les indices en lesquels seront changés les indices qui satisfont à chaque congruence (5).

Substituons donc l'expression (7) dans

$$h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h z + \nu \equiv 0,$$

et nous aurons

$$\left\{\begin{array}{l} h^{p^{\nu-1}}\left(a u^{p^{\nu-1}} + b u^{p^{\nu-2}} + \ldots + l u^{p} + m u + n\right)^{p^{\nu-1}} \\ + h^{p^{\nu-2}}\left(a u^{p^{\nu-1}} + b u^{p^{\nu-2}} + \ldots + m u + n\right)^{p^{\nu-2}} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + h\left(a u^{p^{\nu-1}} + b u^{p^{\nu-2}} + \ldots + l u^{p} + m u + n\right) + \nu \equiv 0. \end{array}\right.$$

Posons

$$h m + h^{p^{\nu-1}} l^{p^{\nu-1}} + \ldots + h^{p} a^{p} \equiv h',$$

$$h^{p^{\nu-1}} n^{p^{\nu-1}} + h^{p^{\nu-2}} n^{p^{\nu-2}} + \ldots + h n \equiv \beta,$$

$\beta$ étant une racine de $z^p \equiv z$, et la congruence précédente deviendra

$$h'^{p^\nu-1} u^{p^\nu-1} + h'^{p^\nu-2} u^{p^\nu-2} + \ldots + h'u + \beta + v \equiv 0,$$

$h$ et $\beta$ étant indépendants de $v$. Donc la fonction $\Phi$ est invariable par toutes les substitutions (2).

La fonction $\Phi$ est d'ailleurs changée par toute autre substitution, ainsi que nous allons le démontrer.

Donnons-nous une substitution quelconque $(z, \varphi z)$ et prenons la substitution inverse

$$\left(u,\ f_{p^\nu-1} u^{p^\nu-1} + f_{p^\nu-2} u^{p^\nu-2} + \ldots + f_l u^l + \ldots\right).$$

Pour que la substitution $(z, \varphi z)$ ne change pas la fonction $\Phi$, il faut qu'en substituant

$$(8) \qquad z = f_{p^\nu-1} u^{p^\nu-1} + f_{p^\nu-2} u^{p^\nu-2} + \ldots + f_l u^l + \ldots$$

dans les congruences (5), on ait des congruences telles que (6), et cela quel que soit $h$; c'est la condition nécessaire et suffisante.

Substituons l'expression (8) dans

$$h^{p^\nu-1} z^{p^\nu-1} + h^{p^\nu-2} z^{p^\nu-2} + \ldots + hz + v \equiv 0$$

et nous aurons la congruence suivante

$$(9)\quad \left\{\begin{aligned} & h^{p^\nu-1}\left[f_{p^\nu-1}^{p^\nu-1} u^{(p^\nu-1)p^\nu-1} + f_{p^\nu-2}^{p^\nu-1} u^{(p^\nu-2)p^\nu-1} + \ldots + f_l^{p^\nu-1} u^{lp^\nu-1} + \ldots\right] \\ & + h^{p^\nu-2}\left[f_{p^\nu-1}^{p^\nu-2} u^{(p^\nu-1)p^\nu-2} + \ldots + f_l^{p^\nu-2} u^{lp^\nu-2} + \ldots\right] + \ldots \\ & + h^{p^\nu-r}\left[f_{p^\nu-1}^{p^\nu-r} u^{(p^\nu-1)p^\nu-r} + \ldots + f_l^{p^\nu-r} u^{lp^\nu-r} + \ldots\right] + \ldots \\ & + h\left[f_{p^\nu-1} u^{p^\nu-1} + f_{p^\nu-2} u^{p^\nu-2} + \ldots + f_l u^l + \ldots\right] + v \equiv 0. \end{aligned}\right.$$

Parmi les termes de cette congruence, il y a les $\nu$ suivants :

$$\left[h^{p^\nu-1} f_l^{p^\nu-1} + h^{p^\nu-2} f_{lp}^{p^\nu-2} + h^{p^\nu-3} f_{lp^2}^{p^\nu-3} + \ldots + h^{p^\nu-r} f_{lp^r}^{p^\nu-r} + \ldots + h f_{lp^{\nu-1}}\right] u^{lp^\nu-1}$$

$$+ \left[h^{p^\nu-2} f_l^{p^\nu-2} + h^{p^\nu-3} f_{lp}^{p^\nu-3} + h^{p^\nu-4} f_{lp^2}^{p^\nu-4} + \ldots + h^{p^\nu-r-1} f_{lp^r}^{p^\nu-r-1} + \ldots + h^{p^\nu-1} f_{lp^{\nu-1}}^{p^\nu-1}\right] u^{lp^\nu-2}$$

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

$$+ \left[h^{p^\nu-s} f_l^{p^\nu-s} + h^{p^\nu-s-1} f_{lp}^{p^\nu-s-1} + h^{p^\nu-s-2} f_{lp^2}^{p^\nu-s-2} + \ldots + h^{p^\nu-s-r} f_{lp^r}^{p^\nu-s-r} + \ldots + h^{p^\nu-s+1} f_{lp^{\nu-1}}^{p^\nu-s+1}\right] u^{lp^\nu-s}.$$

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Nous voyons que les coefficients de ces puissances de $u$ sont tous des puissances du premier. Supposons que $l$ ne soit pas une puissance de $p$; pour que la congruence (9) ait la forme des congruences (6), il faut que les coefficients de ces puissances de $u$ soient nuls : ce qu'on exprimera en égalant simplement le premier à zéro et il viendra :

$$(10) \quad h^{p^\nu-1} f_l^{p^\nu-1} + h^{p^\nu-2} f_{lp}^{p^\nu-2} + \ldots + h^{p^\nu-r} f_{lp^r}^{p^\nu-r} + \ldots + h f_{lp^{\nu-1}} \equiv 0;$$

remarquons que $f_l$, $f_{lp}$, $f_{lp^2}$, $f_{lp^{\nu-1}}$ ne figurent pas dans les autres coefficients des puissances de $u$; mais la congruence (10) devant avoir lieu quel que soit $h$, on a

$$f_l \equiv 0, \quad f_{lp} \equiv 0, \quad f_{lp^2} \equiv 0, \ldots, \quad f_{lp^{\nu-1}} \equiv 0.$$

Si au contraire $l$ est une puissance de $p$, les coefficients de $u^{lp^\nu-1}$, $u^{lp^\nu-2}$, etc., ne devront pas être égalés à zéro et l'on n'aura plus à poser la congruence (10). Donc dans l'expression (8), des différents coefficients $f$ il ne reste que ceux dont les indices sont des puissances de $u$; ce qu'il fallait démontrer.

On peut encore former d'une autre manière élégante une fonction invariable par toutes les substitutions (2).

Soient o. $b_1, b_2, \ldots, b_{p^{\nu-1}-1}$ les racines de la congruence

$$z^{p^{\nu-1}} + z^{p^{\nu-2}} + z^{p^{\nu-3}} + \ldots + z^p + z \equiv 0,$$

ou à la congruence identique

$$(11) \quad \left\{ \begin{array}{l} \lambda(z^{p^\nu} - z) \equiv (\lambda^p z^p - \lambda z)(\lambda^p z^p - \lambda z - b_1)(\lambda^p z^p - \lambda z - b_2)\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots (\lambda^p z^p - \lambda z - b_{p^{\nu-1}-1}). \end{array} \right.$$

Désignons par $\alpha_1, \alpha_2, \ldots, \alpha_p$ les racines de la congruence $\lambda^p z^p - \lambda z \equiv 0$, par $\alpha_1 + m$, $\alpha_2 + m, \ldots, \alpha_p + m$ les racines de $\lambda^p z^p \equiv \lambda z + b_1$, par $\alpha_1 + m'$, $\alpha_2 + m', \ldots$ $\alpha_p + m'$ les racines de $\lambda^p z^p \equiv \lambda z + b_2$, et ainsi de suite. Prenons la fonction

$$(12) \quad \left\{ \begin{array}{l} x_{\alpha_1} x_{\alpha_2} x_{\alpha_3} \ldots x_{\alpha_p} + x_{\alpha_1+m} x_{\alpha_2+m} \ldots x_{\alpha_p+m} \\ \qquad\qquad + x_{\alpha_1+m'} x_{\alpha_2+m'} \ldots + x_{\alpha_p+m'} + \ldots; \end{array} \right.$$

on peut, dans la congruence identique (11), donner $p^\nu - 1$ valeurs à $\lambda$; mais si $e$ est racine de $z^{p-1} \equiv 1$, $\lambda = \lambda_1$ et $\lambda = \lambda_1 e$ donnent la même décomposition en facteurs; il y a donc $\frac{p^\nu - 1}{p-1}$ de ces décompositions, et à chacune de ces décompositions correspond une fonction telle que (12). Pour obtenir ces $\frac{p^\nu - 1}{p-1}$ fonctions, il suffit de faire sur la fonction (12) les substitutions

$$(z, z), \quad (z, \omega z), \quad (z, \omega^2 z), \ldots, \quad \left(z, \omega^{\frac{p^\nu - p}{p-1}} z\right),$$

$\omega$ étant une racine primitive de $z^{p^\nu - 1} \equiv 1$; formons une fonction symétrique $\Psi$ de ces fonctions et nous aurons une fonction invariable par toutes les substitutions (2).

Remarquons d'abord que l'une des fonctions qui composent $\Psi$ est la fonction (12), et que toutes les autres sont représentées par

$$\begin{array}{l} x_{a\alpha_1} x_{a\alpha_2} \ldots x_{a\alpha_p} + x_{a(\alpha_1+m)} x_{a(\alpha_2+m)} \ldots x_{a(\alpha_p+m)} \\ \qquad + x_{a(\alpha_1+m')} x_{a(\alpha_2+m')} \ldots x_{a(\alpha_p+m')} + \ldots \end{array}$$

Faisons la substitution (2); les indices $\alpha_1, \alpha_2, \ldots, \alpha_p$ seront changés en

$$(13)\quad \begin{cases} A\alpha_1^{p^\nu-1} + B\alpha_1^{p^\nu-2} + \ldots + H\alpha_1 + L, \\ A\alpha_2^{p^\nu-1} + B\alpha_2^{p^\nu-2} + \ldots + H\alpha_2 + L, \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

et puisque chacune de ces quantités $\alpha$ satisfait à $\lambda^p\alpha^p - \lambda\alpha \equiv 0$ ou $\alpha^p \equiv \frac{1}{\lambda}\alpha$, les quantités (13) peuvent se mettre sous la forme

$$R\alpha_1 + S,\quad R\alpha_2 + S,\quad R\alpha_3 + S, \ldots,$$

et les indices $\alpha_1 + m$, $\alpha_2 + m$, $\alpha_3 + m, \ldots$, seront changés en

$$R\alpha_1 + S + M,\quad R\alpha_2 + S + M,\quad R\alpha_3 + S + M, \ldots$$

D'où il suit évidemment que les fonctions qui composent $\Psi$ s'échangent entre elles par la substitution (2).

On pourrait encore démontrer que la fonction $\Psi$ est changée par toute substitution qui n'est pas de la forme (2).

Comme précédemment, désignons par $\alpha^{1,1}, \alpha^{1,2}, \ldots, \alpha^{1,p^\nu-1}$ les racines de $z^{p^\nu} \equiv z$ dues au premier facteur du second membre de (3), par $\alpha^{2,1}, \alpha^{2,2}, \ldots, \alpha^{2,p^\nu-1}$ les racines dues au second, et ainsi de suite. On obtiendra une des fonctions qui composent $\Phi$ en formant une fonction symétrique des produits des variables dont les indices sont donnés par les lignes horizontales de ce tableau :

$$(a)\quad \begin{cases} \alpha^{1,1}, & \alpha^{1,2}, & \alpha^{1,3}, \ldots, & \alpha^{1,p^\nu-1}, \\ \alpha^{2,1}, & \alpha^{2,2}, & \alpha^{2,3}, \ldots, & \alpha^{2,p^\nu-1}, \\ \ldots & \ldots & \ldots & \ldots \\ \alpha^{p,1}, & \alpha^{p,2}, & \alpha^{p,3}, \ldots, & \alpha^{p,p^\nu-1}. \end{cases}$$

Multiplions les indices du tableau $(a)$ par $m'$, nous aurons cet autre

tableau

$$(a')\quad \begin{cases} m'\alpha^{1,1}, & m'\alpha^{1,2}, & m'\alpha^{1,3},\ldots, & m'\alpha^{1,p^\nu-1},\\ m'\alpha^{2,1}, & m'\alpha^{2,2}, & m'\alpha^{2,3},\ldots, & m'\alpha^{2,p^\nu-1},\\ \ldots & \ldots & \ldots & \ldots\\ m'\alpha^{p,1}, & m'\alpha^{p,2}, & m'\alpha^{p,3},\ldots, & m'\alpha^{p,p^\nu-1}. \end{cases}$$

On obtiendra encore une des fonctions qui composent $\Phi$ en prenant la même fonction symétrique des produits des variables dont les indices sont donnés par les lignes horizontales du tableau $(a')$.

Remarquons ensuite qu'il y a une et une seule racine de la congruence $z^p = z + b_\nu$ qui appartient à la congruence

$$h^{p^\nu-1} z^{p^\nu-1} + h^{p^\nu-2} z^{p^\nu-2} + \ldots + hz + a = 0.$$

D'après cela, si dans le tableau $(a)$ on a disposé convenablement les termes dans chaque ligne horizontale, les lignes verticales représenteront les racines de $z^p - z - b_\nu = 0$. Alors en prenant une fonction symétrique des produits des variables données par les lignes verticales du tableau $(a)$, on aura une fonction qui compose $\Psi$; on aura de même les autres fonctions qui composent $\Psi$ en agissant semblablement sur les tableaux tels que $(a')$.

*Nota.* — Soient $\Psi$ et $\Psi'$ deux fonctions invariables par les substitutions $(2)$ et soit $\chi$ la fonction des mêmes variables qui a deux valeurs. Si $p$ est différent de $2$, la fonction $\Psi + \Psi'\chi$ a un nombre de valeurs double de celui de $\Psi$.

*Étude des substitutions* $\left(z, \lambda_{\nu-1} z^{p^{\nu-1}} + \lambda_{\nu-2} z^{p^{\nu-2}} + \ldots + \lambda_1 z^p + \lambda_0 z\right)$.

Si on laisse immobile la variable $x_0$, les seules substitutions qui laissent invariables les fonctions que nous venons de considérer sont données par l'expression

$$(14)\qquad \left(z, \lambda_{\nu-1} z^{p^{\nu-1}} + \lambda_{\nu-2} z^{p^{\nu-2}} + \ldots + \lambda_1 z^p + \lambda_0 z\right),$$

et nous allons étudier ces substitutions.

Désignons par $\omega$ une racine d'une congruence irréductible du degré $\nu$; toutes les racines de la congruence $z^{p^\nu} \equiv z$ sont données par l'expression $a_0 + a_1\omega + a_2\omega^2 + \ldots + a_{\nu-1}\omega^{\nu-1}$, $a_0$, $a_1, \ldots$, $a_{\nu-1}$ étant des entiers réels pris par rapport au module $p$. Désignons ensuite par $u_0$, $u_1$, $u_2, \ldots$, $u_{\nu-1}$ les valeurs en lesquelles les indices $1$, $\omega$, $\omega^2, \ldots$, $\omega^{\nu-1}$ sont changés par la substitution (14), nous aurons les congruences :

$$(15)\quad \begin{cases} \lambda_{\nu-1} + \lambda_{\nu-2} + \lambda_{\nu-3} + \ldots + \lambda_1 + \lambda_0 \equiv u_0, \\ \omega^{p^{\nu-1}}\lambda_{\nu-1} + \omega^{p^{\nu-2}}\lambda_{\nu-2} + \omega^{p^{\nu-3}}\lambda_{\nu-3} + \ldots + \omega^p\lambda_1 + \omega\lambda_0 \equiv u_1, \\ \omega^{2p^{\nu-1}}\lambda_{\nu-1} + \omega^{2p^{\nu-2}}\lambda_{\nu-2} + \omega^{2p^{\nu-3}}\lambda_{\nu-3} + \ldots + \omega^{2p}\lambda_1 + \omega^2\lambda_0 \equiv u_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \omega^{(\nu-1)p^{\nu-1}}\lambda_{\nu-1} + \omega^{(\nu-1)p^{\nu-2}}\lambda_{\nu-2} + \omega^{(\nu-1)p^{\nu-3}}\lambda_{\nu-3} + \ldots + \omega^{\nu-1}\lambda_0 \equiv u_{\nu-1}, \end{cases}$$

Au moyen de ces congruences, on pourra tirer les valeurs de $\lambda_{\nu-1}$, $\lambda_{\nu-2}, \ldots$, $\lambda_0$, et il s'agit de prendre les quantités $u_0$, $u_1$, $u_2, \ldots$, $u_{\nu-1}$ de telle façon que l'expression (14) soit bien une substitution.

Multiplions les congruences (15) respectivement par les entiers $a_0$, $a_1, \ldots$, $a_{\nu-1}$ et ajoutons, nous aurons

$$\begin{cases} \left(a_0 + a_1\omega + a_2\omega^2 + \ldots + a_{\nu-1}\omega^{\nu-1}\right)^{p^{\nu-1}}\lambda_{\nu-1} \\ + \left(a_0 + a_1\omega + \ldots + a_{\nu-1}\omega^{\nu-1}\right)^{p^{\nu-2}}\lambda_{\nu-2} + \ldots\ldots \\ + \left(a_0 + a_1\omega + \ldots + a_{\nu-1}\omega^{\nu-1}\right)^{p}\lambda_1 \\ + \left(a_0 + a_1\omega + \ldots + a_{\nu-1}\omega^{\nu-1}\right)\lambda_0 \\ \equiv a_0 u_0 + a_1 u_1 + \ldots + a_{\nu-1}u_{\nu-1}. \end{cases}$$

D'après cela, pour que l'expression (14) représente une substitution, il faut qu'en donnant aux quantités $a_0$, $a_1, \ldots$, $a_{\nu-1}$ toutes les valeurs dont elles sont susceptibles, l'expression $a_0 u_0 + a_1 u_1 + \ldots + a_{\nu-1}u_{\nu-1}$ prenne $p^\nu$ valeurs différentes ; à cet effet nous prendrons $u_0$, $u_1, \ldots$, $u_{\nu-1}$ de la manière suivante.

Nous prendrons d'abord pour $u_0$ une quelconque des racines de la

congruence $z^{p^\nu-1}\equiv 1$. Formons la congruence

$$z(z-u_0)(z-2u_0)(z-3u_0)\ldots(z-\overline{p-1}\,u_0)\equiv 0.$$

ou

$$z^p-u_0^{p-1}z\equiv 0;$$

nous prendrons pour $u_1$ une quelconque des valeurs qui ne satisfont pas à cette congruence, c'est-à-dire qui ne sont pas de la forme $\alpha_0 u_0$. $\alpha_0$ étant un nombre entier.

Formons la congruence

$$\begin{aligned}(z^p-u_0^{p-1}z)\left[z^p-u_0^{p-1}z-(u_1^p-u_0^{p-1}u_1)\right]\\ \times\left[z^p-u_0^{p-1}z-2(u_1^p-u_0^{p-1}u_1)\right]\ldots\\ \times\left[z^p-u_0^{p-1}z-\overline{p-1}(u_1^p-u_0^{p-1}u_1)\right]\equiv 0\end{aligned}$$

qui peut se mettre sous la forme

$$z^{p^2}+\mathrm{M}z^p+\mathrm{N}\equiv 0;$$

nous prendrons pour $u_2$ une quelconque des $p^\nu-p^2$ quantités qui ne satisfont pas à cette dernière congruence; $u_2$ sera donc assujetti à ne pas être de la forme $\alpha_0 u_0+\alpha_1 u_1$, $\alpha_0$ et $\alpha_1$ étant deux entiers.

Ayant ainsi fixé les valeurs de $u_0$, $u_1,\ldots, u_{\nu-1}$, l'expression $a_0u_0+a_1u_1+\ldots+a_{\nu-1}u_{\nu-1}$ renferme évidemment $p^\nu$ quantités différentes; car $a_0u_0$ est susceptible de $p$ valeurs; $u_1$ n'est pas de la forme $\alpha_0u_0$; donc $a_0u_0+a_1u_1$ est susceptible de $p^2$ valeurs, et ainsi de suite.

D'ailleurs si $u_0, u_1,\ldots, u_{\nu-1}$ sont pris d'autre sorte et que l'on ait par exemple $u_k=\alpha_0u_0+\alpha_1u_1+\ldots+\alpha_{k-1}u_{k-1}$, il est clair que l'on n'a plus $p^\nu$ valeurs distinctes pour l'expression $a_0u_0+a_1u_1+\ldots+a_{\nu-1}u_{\nu-1}$, et par conséquent l'expression (14) ne représente plus une substitution. Donc $u_0, u_1,\ldots, u_{\nu-1}$ doivent être déterminés comme nous l'avons fait.

Nous avons vu que l'on peut donner $p^\nu-1$ valeurs à $u_0$, que la va-

leur de $u_0$ étant fixée, on peut choisir pour $u_1$ entre $p^\nu - p$ valeurs, puis pour $u_2$ on peut choisir entre $p^\nu - p^2$ valeurs, etc, et enfin pour $u_{\nu-1}$ on peut choisir entre $p^\nu - p^{\nu-1}$ valeurs; donc le nombre des substitutions (14) est

$$(p^\nu - 1)(p^\nu - p)(p^\nu - p^2)\ldots(p^\nu - p^{\nu-1});$$

donc aussi le nombre des valeurs de la fonction de $p^\nu$ quantités invariable par toutes les substitutions

$$(z,\ Az^{p^{\nu-1}} + Bz^{p^{\nu-2}} + \ldots + Hz + L)$$

est

$$\frac{1.2.3\ldots(p^\nu - 1)}{(p^\nu - p^{\nu-1})(p^\nu - p^{\nu-2})\ldots(p^\nu - p)(p^\nu - 1)}.$$

Soient $\omega_0, \omega_1, \omega_2, \ldots, \omega_{\nu-1}$, $\nu$ quantités obtenues comme $u_0, u_1, \ldots, u_{\nu-1}$; toutes les racines de $z^{p^\nu} \equiv z$ sont renfermées dans la formule $a_0\omega_0 + a_1\omega_1 + \ldots + a_{\nu-1}\omega_{\nu-1}$. Si donc, au lieu de poser les congruences (15), on pose les congruences

$$(16)\quad \begin{cases} \omega_0^{p^{\nu-1}}\lambda_{\nu-1} + \omega_0^{p^{\nu-2}}\lambda_{\nu-2} + \ldots + \omega_0^{p}\lambda_1 + \omega_0\lambda_0 \equiv u_0, \\ \omega_1^{p^{\nu-1}}\lambda_{\nu-1} + \omega_1^{p^{\nu-2}}\lambda_{\nu-2} + \ldots + \omega_1^{p}\lambda_1 + \omega_1\lambda_0 \equiv u_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \omega_{\nu-1}^{p^{\nu-1}}\lambda_{\nu-1} + \omega_{\nu-1}^{p^{\nu-2}}\lambda_{\nu-2} + \ldots + \omega_{\nu-1}^{p}\lambda_1 + \omega_{\nu-1}\lambda_0 \equiv u_{\nu-1}, \end{cases}$$

on en tirera

$$(b)\quad \begin{cases} (a_0\omega_0 + a_1\omega_1 + \ldots + a_{\nu-1}\omega_{\nu-1})^{p^{\nu-1}}\lambda_{\nu-1} \\ + (a_0\omega_0 + a_1\omega_1 + \ldots + a_{\nu-1}\omega_{\nu-1})^{p^{\nu-2}}\lambda_{\nu-2} + \ldots\ldots \\ + (a_0\omega_0 + \ldots + a_{\nu-1}\omega_{\nu-1})\lambda_0 \equiv a_0u_0 + a_1u_1 + \ldots + a_{\nu-1}u_{\nu-1}, \end{cases}$$

et les valeurs de $u_0, u_1, \ldots, u_{\nu-1}$ devront encore être prises comme nous l'avons fait ci-dessus.

Considérons les substitutions (14) qui laissent immobiles les $p^k$ va-

riables dont les indices sont représentés par l'expression

$$(17)\qquad a_0\omega_0 + a_1\omega_1 + \ldots + a_{k-1}\omega_{k-1}.$$

Je dis que la fonction qui est invariable par les substitutions (14) est transitive par rapport aux $p^\nu - p^k$ variables qui ne sont pas comprises dans la forme (17).

En effet, dans les congruences (16), faisons $u_0 \equiv \omega_0$, $u_1 \equiv \omega_1, \ldots u_{k-1} \equiv \omega_{k-1}$, la substitution (14) laissera alors immobiles les $p_k$ variables (17), puisque la congruence ($b$) deviendra

$$\left\{\begin{aligned} &(a_0\omega_0 + a_1\omega_1 + \ldots + a_{\nu-1}\omega_{\nu-1})^{p^{\nu-1}}\lambda_{\nu-1} \\ &+ (a_0\omega_0 + a_1\omega_1 + \ldots + a_{\nu-1}\omega_{\nu-1})^{p^{\nu-2}}\lambda_{\nu-2} + \ldots \\ &+ (a_0\omega_0 + \ldots + a_{\nu-1}\omega_{\nu-1})\lambda_0 \\ &\equiv a_0\omega_0 + \ldots a_{k-1}\omega_{k-1} + a_k u_k + \ldots + a_{\nu-1}u_{\nu-1}. \end{aligned}\right.$$

Pour que la fonction considérée soit transitive par rapport aux $p^\nu - p^k$ variables autres que les variables (17), il suffit que l'on puisse changer une de ces variables en une quelconque des $p^\nu - p^k - 1$ autres; or on changera l'indice déterminé

$$a_0\omega_0 + a_1\omega_1 + \ldots + a_{k-1}\omega_{k-1} + a_k\omega_k,$$

dans lequel $a_k$ est incongru à zéro, en l'indice

$$a'_0\omega_0 + a'_1\omega_1 + \ldots + a'_{k-1}\omega_{k-1} + \ldots + a'_{\nu-1}\omega_{\nu-1},$$

en satisfaisant à la congruence

$$(18)\qquad a_0\omega_0 + \ldots + a_{k-1}\omega_{k-1} + a_k u_k \equiv a'_0\omega_0 + a'_1\omega_1 + \ldots + a'_{\nu-1}\omega_{\nu-1};$$

$a_k$ est différent de zéro, et parmi les quantités $a'_k, a'_{k+1}, \ldots, a'_{\nu-1}$, il y en a au moins une qui est différente de zéro; donc la valeur de $u_k$ donnée par la congruence (18) est convenable, puisque l'on peut prendre pour $u_k$ toute expression qui n'est pas de la forme (17). On voit donc que l'on peut changer une des $p^\nu - p^k$ variables qui ne sont

pas de la forme (17) en une quelconque des $p^\nu - p^k - 1$ autres de ces variables; donc la fonction considérée est transitive par rapport à ces $p^\nu - p^k$ variables.

D'après cela, soient $\omega_0, \omega_1, \ldots, \omega_{\nu-1}$, $\nu$ racines de la congruence $z^{p^\nu} \equiv z$, telles que l'on n'ait pas $\omega_k \equiv \alpha_0 \omega_0 + \alpha_1 \omega_1 + \ldots + \alpha_{k-1} \omega_{k-1}$, $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$ étant des entiers, la fonction de $p^\nu$ variables qui n'est pas changée par toutes les substitutions

$$(19) \qquad \left(z, \quad \lambda_{\nu-1} z^{p^{\nu-1}} + \lambda_{\nu-2} z^{p^{\nu-2}} + \ldots + \lambda_0 z + m\right),$$

est transitive par rapport à ses $p^\nu$ variables, puis transitive par rapport aux $p^\nu - 1$ variables autres que $x_0$, puis transitive par rapport aux $p^\nu - p$ variables dont les indices ne sont pas de la forme $\alpha_0 \omega_0$, puis transitive par rapport aux $p^\nu - p^2$ variables dont les indices ne sont pas de la forme $\alpha_0 \omega_0 + \alpha_1 \omega_1$, etc., et enfin transitive par rapport aux $p^\nu - p^{\nu-1}$ variables dont les indices ne sont pas de la forme

$$\alpha_0 \omega_0 + \alpha_1 \omega_1 + \ldots + \alpha_{\nu-2} \omega_{\nu-2}.$$

La fonction invariable par toutes les substitutions (19) est donc en général deux fois transitive; dans le cas de $p = 2$, cette fonction est trois fois transitive.

Désignons par D le déterminant

$$\begin{vmatrix} \omega_0^{p^{\nu-1}}, & \omega_0^{p^{\nu-2}}, \ldots, & \omega_0^{p}, & \omega_0 \\ \omega_1^{p^{\nu-1}}, & \omega_1^{p^{\nu-2}}, \ldots, & \omega_1^{p}, & \omega_1 \\ \ldots & \ldots & \ldots & \ldots \\ \omega_{\nu-1}^{p^{\nu-1}}, & \omega_{\nu-1}^{p^{\nu-2}}, \ldots, & \omega_{\nu-1}^{p}, & \omega_{\nu-1} \end{vmatrix}.$$

Les congruences (16) nous donneront

$$\lambda_\varepsilon \equiv \frac{1}{D}\left(u_0 \frac{dD}{d\omega_0^{p^\varepsilon}} + u_1 \frac{dD}{d\omega_1^{p^\varepsilon}} + \ldots + u_{\nu-1} \frac{dD}{d\omega_{\nu-1}^{p^\varepsilon}}\right),$$

et par conséquent nous aurons, en posant

$$\frac{dD}{d\omega_r} = h_r$$

et par suite

$$\frac{dD}{d\omega_r^{p^\varepsilon}} \equiv \left(\frac{dD}{d\omega_r}\right)^{p^\varepsilon} = h_r^{p^\varepsilon}$$

la congruence

$$(20)\quad \begin{cases} \lambda_{\nu-1} z^{p^{\nu-1}} + \lambda_{\nu-2} z^{p^{\nu-2}} + \ldots + \lambda_1 z^p + \lambda_0 z \\ \equiv \frac{u_0}{D}\left(h_0^{p^{\nu-1}} z^{p^{\nu-1}} + h_0^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h_0 z\right) \\ + \frac{u_1}{D}\left(h_1^{p^{\nu-1}} z^{p^{\nu-1}} + h_1^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h_1 z\right) + \ldots \\ + \frac{u_{\nu-1}}{D}\left(h_{\nu-1}^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h_{\nu-1} z\right). \end{cases}$$

Si la substitution (14) ne permute aucune des $p^k$ variables

$$x_{a_0\omega_0 + a_1\omega_1 + \ldots + a_{k-1}\omega_{k-1}}$$

on voit facilement que l'on a

$$\begin{cases} \lambda_{\nu-1} z^{p^{\nu-1}} + \ldots + \lambda_1 z^p + \lambda_0 z \\ \equiv z + \frac{u_k - \omega_k}{D}\left(h_k^{p^{\nu-1}} z^{p^{\nu-1}} + h_k^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h_k z\right) \\ + \frac{u_{k+1} - \omega_{k+1}}{D}\left(h_{k+1}^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h_{k+1} z\right) + \ldots \\ + \frac{u_{\nu-1} - \omega_{\nu-1}}{D}\left(h_{\nu-1}^{p^{\nu-1}} z^{p^{\nu-1}} + h_{\nu-1}^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + h_{\nu-1} z\right). \end{cases}$$

En particulier, si on fait $k = \nu - 1$, on aura

$$\lambda_{\nu-1} z^{p^{\nu-1}} + \ldots + \lambda_1 z^p + \lambda_0 z$$
$$\equiv z + a\left(h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + hz\right),$$

et par conséquent les substitutions qui s'effectuent sur $p^\nu - p^{\nu-1}$ variables sont données par l'expression

$$\left[z,\ z + a\left(h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + hz\right)\right].$$

Si on élève D à la puissance $p^{ieme}$, il est aisé de voir que D reste le même ou change de signe seulement; on a donc $D^p \pm D \equiv 0 \pmod{p}$: ainsi dans le cas de $p = 2$, on a $D \equiv 1 \pmod{2}$.

*Application à la fonction deux fois transitive de neuf quantités qui a 840 valeurs.*

Proposons-nous de déterminer la fonction deux fois transitive de neuf quantités qui a $\frac{1.2.3.4.5.6.7.8}{(3^2-1)(3^2-3)} = 840$ valeurs, et qui est invariable par toutes les substitutions

$$(a) \qquad (z, \lambda_1 z^3 + \lambda_0 z + m).$$

Désignons par $\omega$ une racine de la congruence irréductible

$$\omega^2 + 2\omega + 2 \equiv 0 \pmod{3},$$

nous aurons

$$z^{3^2} - z \equiv (z^3 + z)(z^3 + z + 1)(z^3 + z + 2),$$

et les racines de $z^{3^2} - z \equiv 0$ dues à ces trois facteurs sont

$$1^\circ \quad 0,\ 1+\omega,\ 2+2\omega; \quad 2^\circ \quad 1,\ 2+\omega,\ 2\omega; \quad 3^\circ \quad 2,\ \omega,\ 1+2\omega.$$

Nous aurons donc la fonction cherchée en formant une fonction symétrique de ces quatre fonctions :

$$\left\{\begin{array}{l} x_0 x_{1+\omega} x_{2+2\omega} + x_1 x_{2+\omega} x_{2\omega} + x_2 x_\omega x_{1+2\omega}, \\ x_0 x_{1+2\omega} x_{2+\omega} + x_\omega x_1 x_{2+2\omega} + x_{2\omega} x_{1+\omega} x_2, \\ x_0 x_2 x_1 + x_{1+\omega} x_\omega x_{2+\omega} + x_{2+2\omega} x_{1+2\omega} x_{2\omega}, \\ x_0 x_{2\omega} x_\omega + x_{1+2\omega} x_{1+\omega} x_1 + x_{2+\omega} x_2 x_{2+2\omega}. \end{array}\right.$$

Nous déterminerons $\lambda_1$ et $\lambda_0$ par les congruences

$$\left.\begin{array}{r} \lambda_1 + \lambda_0 \equiv u_0, \\ \omega^3 \lambda_1 + \omega\lambda_0 \equiv u_1, \end{array}\right\} \pmod{3},$$

et les substitutions $(a)$ sont données par l'expression

$$[z, (\omega^3 u_0 + \omega^6 u_1) z^3 + (\omega u_0 + \omega^2 u_1) z + m],$$

$u_0$ étant un nombre quelconque différent de zéro, et $u_1$ étant un nombre quelconque autre que o, $u_0$, $2u_0$.

*Application à la fonction trois fois transitive de huit quantités qui a 30 valeurs.*

Formons ensuite la fonction trois fois transitive de huit quantités, qui a $\frac{1.2.3.4.5.6.7}{(2^3-1)(2^3-2)(2^3-2^2)} = 30$ valeurs, et qui est invariable par toutes les substitutions

$$(b) \qquad (z, \lambda_2 z^4 + \lambda_1 z^2 + \lambda_0 z + m).$$

Soit $\omega$ une racine de la congruence irréductible

$$\omega^3 + \omega + 1 \equiv 0 \pmod{2},$$

$\omega$ est racine primitive de $z^7 \equiv 1$. On a la congruence

$$z^{2^3} - z \equiv (z^4 + z^2 + z)(z^4 + z^2 + z + 1),$$

et les racines de $z^{2^3} - z \equiv 0$ dues à ces deux facteurs sont

$$0, \quad \omega, \quad \omega^2, \quad \omega + \omega^2,$$

et

$$1, \quad 1 + \omega, \quad 1 + \omega^2, \quad 1 + \omega + \omega^2.$$

On a d'autre part

$$z^{2^3} - z \equiv (z^2 + z)(z^2 + z + \omega)(z^2 + z + \omega^2)(z^2 + z + \omega + \omega^2),$$

et les racines dues à ces facteurs sont

$$1^\circ\ 0, 1; \quad 2^\circ\ \omega, 1 + \omega; \quad 3^\circ\ \omega^2, 1 + \omega^2; \quad 4^\circ\ \omega + \omega^2, 1 + \omega + \omega^2.$$

D'après cela, faisons sur la fonction

$$x_0 x_\omega x_{\omega^2} x_{\omega+\omega^2} + x_1 x_{1+\omega} x_{1+\omega^2} x_{1+\omega+\omega^2}$$

la substitution $(z, \omega z)$ ou

$$(x_1 x_\omega x_{\omega^2} x_{1+\omega} x_{\omega+\omega^2} x_{1+\omega+\omega^2} x_{1+\omega^2}),$$

et ses puissances, nous aurons les sept fonctions :

$$\left\{\begin{array}{l}
x_0 x_\omega x_{\omega^2} x_{\omega+\omega^2} + x_1 x_{1+\omega} x_{1+\omega^2} x_{1+\omega+\omega^2}, \\
x_0 x_{\omega^2} x_{1+\omega} x_{1+\omega+\omega^2} + x_\omega x_{\omega+\omega^2} x_1 x_{1+\omega^2}, \\
x_0 x_{1+\omega} x_{\omega+\omega^2} x_{1+\omega^2} + x_{\omega^2} x_{1+\omega-\omega^2} x_\omega x_1, \\
x_0 x_{\omega+\omega^2} x_{1+\omega+\omega^2} x_1 + x_{1+\omega} x_{1+\omega^2} x_{\omega^2} x_\omega, \\
x_0 x_{1+\omega+\omega^2} x_{1+\omega^2} x_\omega + x_{\omega+\omega^2} x_1 x_{1+\omega} x_{\omega^2}, \\
x_0 x_{1+\omega^2} x_1 x_{\omega^2} + x_{1+\omega+\omega^2} x_\omega x_{\omega+\omega^2} x_{1+\omega}, \\
x_0 x_1 x_\omega x_{1+\omega} + x_{1+\omega^2} x_{\omega^2} x_{1+\omega+\omega^2} x_{\omega+\omega^2},
\end{array}\right.$$

et toute fonction symétrique de ces fonctions est invariable par les substitutions $(b)$.

En second lieu considérons la fonction

$$x_0 x_1 + x_\omega x_{1+\omega} + x_{\omega^2} x_{1+\omega^2} + x_{\omega+\omega^2} x_{1+\omega+\omega^2},$$

et faisons sur cette fonction la substitution circulaire $(z, \omega z)$ et ses puissances, nous aurons les sept fonctions suivantes :

$$\left\{\begin{array}{l}
x_0 x_1 + x_\omega x_{1+\omega} + x_{\omega^2} x_{1+\omega^2} + x_{\omega+\omega^2} x_{1+\omega+\omega^2}, \\
x_0 x_\omega + x_{\omega^2} x_{\omega+\omega^2} + x_{1+\omega} x_1 + x_{1+\omega+\omega^2} x_{1+\omega^2}, \\
x_0 x_{\omega^2} + x_{1+\omega} x_{1+\omega+\omega^2} + x_{\omega+\omega^2} x_\omega + x_{1+\omega^2} x_1, \\
x_0 x_{1+\omega} + x_{\omega+\omega^2} x_{1+\omega^2} + x_{1+\omega+\omega^2} x_{\omega^2} + x_1 x_\omega, \\
x_0 x_{\omega+\omega^2} + x_{1+\omega+\omega^2} x_1 + x_{1+\omega^2} x_{1+\omega} + x_\omega x_{\omega^2}, \\
x_0 x_{1+\omega+\omega^2} + x_{1+\omega^2} x_\omega + x_1 x_{\omega+\omega^2} + x_{\omega^2} x_{1+\omega}, \\
x_0 x_{1+\omega^2} + x_1 x_{\omega^2} + x_\omega x_{1+\omega+\omega^2} + x_{1+\omega} x_{\omega+\omega^2};
\end{array}\right.$$

formons une fonction symétrique de ces fonctions, et nous aurons encore une fonction invariable par toutes les substitutions $(b)$.

Actuellement déterminons dans l'expression $(b)$ les coefficients $\lambda_2$, $\lambda_1$, $\lambda_0$; pour cela nous poserons les congruences

$$\left.\begin{aligned} \lambda_2 + \lambda_1 + \lambda_0 &\equiv u_0, \\ \omega^4\lambda_2 + \omega^2\lambda_1 + \omega\lambda_0 &\equiv u_1, \\ \omega\lambda_2 + \omega^4\lambda_1 + \omega^2\lambda_0 &\equiv u_2, \end{aligned}\right\} \pmod{2}.$$

et nous en tirerons

$$\left.\begin{aligned} \lambda_2 &\equiv u_0 + \omega u_1 + (\omega + \omega^2) u_2, \\ \lambda_1 &\equiv u_0 + (\omega + \omega^2) u_1 + \omega^2 u_2, \\ \lambda_0 &\equiv u_0 + \omega^2 u_1 + \omega u_2, \end{aligned}\right\} \pmod{2}$$

Par conséquent les substitutions $(b)$ sont données par l'expression

$$(c)\qquad \left\{\begin{aligned} &[z, (u_0 + \omega u_1 + \omega^4 u_2) z^4 + (u_0 + \omega^4 u_1 + \omega^2 u_2) z^2 \\ &\qquad + (u_0 + \omega^2 u_1 + \omega u_2) z + m], \end{aligned}\right.$$

$u_0$, $u_1$, $u_2$ étant trois quantités différentes entre elles et différentes de zéro et $u_2$ étant de plus assujetti à n'être pas $= u_0 + u_1$.

Il y a deux fonctions deux fois transitives distinctes de huit quantités qui ont 240 valeurs, et il est remarquable que la fonction de huit quantités qui a 30 valeurs est invariable par les substitutions qui ne changent pas ces deux fonctions.

L'une de ces fonctions deux fois transitives est invariable par les substitutions $\left(z, az^{2^\alpha} + b\right)$, $\alpha$ étant quelconque, et ces substitutions font évidemment partie des substitutions $(c)$.

La seconde de ces fonctions est invariable par les substitutions

$$\left(z, \frac{Az + B}{Cz + D}\right) \pmod{7},$$

$AD - BC$ étant résidu quadratique et les huit variables étant désignées par $x_0$, $x_1$, $x_2$, $x_3$, $x_4$, $x_5$, $x_6$, $x_\infty$. D'après un théoreme facile à dé-

montrer, toutes ces substitutions sont des dérivées des deux substitutions

$$(e) \qquad (z, z+1),$$

$$(f) \qquad \left(z, \frac{z}{z+1}\right).$$

Remplaçons donc les variables

$$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_\infty$$

respectivement par

$$x_1, x_\omega, x_{\omega^2}, x_{\omega^3}, x_{\omega^4}, x_{\omega^5}, x_{\omega^6}, x_0,$$

$\omega$ étant une racine de $z^7 \equiv 1$, de sorte que nous reprenons nos notations précédentes pour représenter les huit quantités.

La substitution $(z, z+1)$ est remplacée par

$$(\omega^z, \omega^{z+1}) \quad \text{ou} \quad (z, \omega z);$$

la substitution $(f)$ devient par le même changement de notation, en prenant les exposants suivant le module 7,

$$(x_0\, x_\omega\, x_{\omega^{\frac{1}{2}}}\, x_{\omega^{\frac{1}{3}}}\, x_{\omega^{\frac{1}{4}}}\, x_{\omega^{\frac{1}{5}}}\, x_{\omega^{\frac{1}{6}}})$$

ou

$$(g) \qquad [z, (\omega + \omega^2) z^4 + (\omega^2 + \omega^4) z^2 + (\omega^4 + 1) z + \omega]:$$

donc elle fait partie des substitutions $(c)$ et l'on voit que la fonction qui a 30 valeurs est invariable par toutes les substitutions qui ne changent pas la fonction deux fois transitive considérée.

Quand on a eu le soin d'écrire la substitution $(g)$ tout à fait comme nous venons de le faire, les puissances 2^e^, 3^e^, ..., 6^e^ s'obtiennent en remplaçant $\omega$ respectivement par $\omega^{\frac{1}{2}} = \omega^4$, $\omega^{\frac{1}{3}} = \omega^5$, $\omega^{\frac{1}{4}} = \omega^2$, $\omega^{\frac{1}{5}} = \omega^3$, $\omega^{\frac{1}{6}} = \omega^6$; de sorte que les puissances de cette substitution sont ren-

fermées dans l'expression

$$[z, (a+a^2)z^4 + (a^2+a^4)z^2 + (a^4+1)z + a]$$

$a$ étant quelconque, excepté zéro.

*Etude des substitutions* $\left[z, z + a\left(h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + hz\right)\right]$.

D'après ce que nous avons reconnu ci-dessus, toutes les substitutions de la forme $\left(z, \lambda_{\nu-1} z^{p^{\nu-1}} + \ldots + \lambda_0 z\right)$ qui s'effectuent sur $p^\nu - p^{\nu-1}$ quantités, sont renfermées dans l'expression

$$(a) \qquad \left[z, z + a(h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + hz)\right].$$

Or on peut, au moyen de ces seules substitutions, déterminer le nombre des valeurs de la fonction de $p^\nu - 1$ quantités qui est invariable pour toutes les subtitutions

$$(b) \qquad \left(z, \lambda_{\nu-1} z^{p^{\nu-1}} + \lambda_{\nu-2} z^{p^{\nu-2}} + \ldots + \lambda_0 z\right)$$

et par conséquent toutes les substitutions $(b)$ sont des dérivées des substitutions $(a)$; c'est ce que nous allons expliquer. Mais, avant tout, disons comment les substitutions $(a)$ se décomposent en cycles.

Comme nous l'avons déjà dit, on a

$$\begin{aligned} h\left(z^{p^\nu} - z\right) \equiv & \left(h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h^p z^p + hz\right) \\ & \times \left(h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + hz + 1\right) \\ & \times \left(h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + hz + 2\right) \ldots \\ & \times \left(h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + hz + p - 1\right), \end{aligned}$$

et par suite toute racine de $z^{p^\nu} \equiv z$ satisfait à la congruence

$$h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + hz \equiv m \pmod{p},$$

$m$ étant un nombre entier convenablement choisi.

La substitution $(a)$ laisse immobiles les $p^{\nu-1}$ quantités dont les indices satisfont à

$$h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + hz \equiv 0.$$

Posons

$$h^{p^{\nu-1}} z^{p^{\nu-1}} + h^{p^{\nu-2}} z^{p^{\nu-2}} + \ldots + hz \equiv \psi z,$$

et l'on trouve facilement que la puissance $k^{\text{ième}}$ de la substitution $(a)$ est

$$\left(z,\ z + \frac{[(1+\psi(a))^k - 1]a}{\psi(a)} \psi z\right).$$

Si $\psi(a)$ est $\equiv 0$, la puissance $k^{\text{ième}}$ de la substitution $(a)$ se réduit à $(z, z + k\psi z)$, et l'on voit par là que $(a)$ est une substitution régulière de $p^\nu - p^{\nu-1}$ quantités composée de $p^{\nu-1} - p^{\nu-2}$ cycles de $p$ quantités.

Supposons $\psi(a) \equiv m$, $m$ étant un nombre entier qui n'est pas nul, et soit $\varepsilon$ le plus petit nombre pour lequel on a

$$[1 + \psi(a)]^\varepsilon \equiv 1;$$

cette congruence pourra toujours être satisfaite si $\psi(a)$ n'est pas $\equiv -1$, et on en conclut que l'expression $(a)$ n'est pas une substitution dans le cas où $\psi(a)$ est $\equiv p - 1$, et que si on a $\psi(a) \equiv m$, $m$ étant différent de zéro et de $p - 1$, l'expression $(a)$ représente une substitution régulière de $p^\nu - p^{\nu-1}$ variables composée de $\dfrac{p^\nu - p^{\nu-1}}{\varepsilon}$ cycles de $\varepsilon$ variables.

Actuellement soient $p^k$ variables dont les indices satisfont à la congruence

$$(c) \qquad z^{p^k} + l_{k-1} z^{p^{k-1}} + l_{k-2} z^{p^{k-2}} + \ldots + l_0 z \equiv \zeta(z) \equiv 0,$$

et soient $x_{z_1}$ et $x_\alpha$ deux quelconques des $p^\nu - p^k$ variables dont les indices ne satisfont pas à $(c)$, et parmi les substitutions $(a)$ ne considérons que celles qui s'effectuent sur ces $p^\nu - p^k$ variables; nous allons faire voir qu'au moyen de ces substitutions, on peut toujours changer $x_{z_1}$ en $x_\alpha$.

Toutes les racines de $(c)$ sont racines de $z^{p^\nu} \equiv z$, et par suite si on ajoute aux racines de la congruence $(c)$ une racine $d$ de $z^{p^\nu} \equiv z$, qui n'appartienne pas à $(c)$, la congruence qui en résulte est

$$(g) \qquad \zeta(z) - \zeta(d) \equiv 0,$$

et son premier membre est un diviseur de $z^{p^\nu} - z$; de même si $e$ est une racine de $z^{p^\nu} \equiv z$ qui n'appartient ni à $(c)$, ni à $(g)$,

$$\zeta(z) - \zeta(e)$$

est un diviseur de $z^{p^\nu} - z$. Comme on peut former ainsi successivement des diviseurs de $z^{p^\nu} - z$, on voit que l'on peut poser

$$z^{p^\nu} - z = \zeta(z).[\zeta(z) + m'][\zeta(z) + m'']\ldots\left[\zeta(z) + m^{(p^{\nu-k}-1)}\right].$$

Alors il arrivera de deux choses l'une : $z_1$ et $\alpha$ satisferont à deux congruences différentes

$$(h) \qquad \zeta(z) + m' \equiv 0, \quad \zeta(z) + m'' \equiv 0,$$

ou bien $z_1$ et $\alpha$ satisferont à une seule de ces deux congruences.

Supposons d'abord que $z_1$ et $\alpha$ satisfassent tous deux à la première congruence $(h)$. Formons les deux congruences

$$(\alpha) \qquad \zeta(z) \equiv 0,$$

$$(\beta) \quad [\zeta(z) + m'][\zeta(z) + 2m'][\zeta(z) + 3m']\ldots[\zeta(z) + (p-1)m'] \equiv 0.$$

Soit $\beta_1$ une racine de $z^{p^\nu} - z \equiv 0$, qui n'appartient ni à $(\alpha)$, ni à $(\beta)$, et formons une congruence qui ait pour racines les racines de $(\alpha)$ augmentées successivement de $0, \beta_1, 2\beta_1, \ldots, (p-1)\beta_1$ ; nous l'écrirons :

$$(\alpha') \quad \zeta(z)[\zeta(z) + r][\zeta(z) + 2r]\ldots[\zeta(z) + (p-1)r] \equiv \theta z \equiv 0.$$

Formons de même une congruence qui ait pour racines les racines

de $(\beta)$ augmentées successivement de $0, \beta_1, 2\beta_1, \ldots (p-1)\beta_1$; elle sera

$$(\beta')\quad [\theta(z)+s][\theta(z)+2s][\theta(z)+3s]..[\theta(z)+(p-1)s] \equiv 0.$$

Soit $\beta_2$ une racine de $z^{p^\nu} \equiv z$ qui n'appartient ni à $(\alpha')$, ni à $(\beta')$, nous formerons de même une congruence $(\alpha'')$ qui ait pour racines les racines de $(\alpha')$ augmentées successivement de $0, \beta_2, 2\beta_2, \ldots, (p-1)\beta_2$,

$$(\alpha'')\qquad z^{p^{k+2}} + q_{k+1} z^{p^{k+1}} + q_k z^{p^k} + \ldots + q_0 z \equiv \lambda(z) \equiv 0,$$

et nous formerons une congruence $(\beta'')$ qui ait les racines de $(\beta')$ augmentées de ces mêmes quantités :

$$(\beta'')\qquad [\lambda(z)+t][\lambda(z)+2t]\ldots[\lambda(z)+(p-1)t] \equiv 0.$$

Et en continuant d'agir ainsi, on finira par former les deux congruences

$$(\text{A})\qquad h^{p^\nu-1} z^{p^\nu-1} + h^{p^\nu-2} z^{p^\nu-2} + \ldots + hz \equiv 0,$$

$$(\text{B})\qquad \left\{\begin{array}{l} \left(h^{p^\nu-1} z^{p^\nu-1} + \ldots + h^p z^p + hz + 1\right) \\ \times \left(h^{p^\nu-1} z^{p^\nu-1} + \ldots + hz + 2\right)\ldots \\ \times \left(h^{p^\nu-1} z^{p^\nu-1} + \ldots + hz + p - 1\right) \equiv 0, \end{array}\right.$$

qui seront telles que les indices des $p^k$ variables qui satisfont à la congruence $(c)$ satisferont à (A) et que $z_1$ et $\alpha$ satisferont à (B).

Supposons ensuite que $z_1$ et $\alpha$ satisfassent respectivement à la première et à la seconde congruence $(h)$. Dans le cas où $m''$ est $\equiv rm'$, $r$ étant un entier, nous voyons que les deux congruences $(h)$ sont renfermées dans la congruence $(\beta)$, et par conséquent la méthode que nous venons d'exposer nous conduira encore aux deux congruences (A) et (B) qui jouiront des mêmes propriétés.

Supposons donc que l'on n'ait pas $m'' \equiv rm'$; formons la congruence :

$$(\alpha_1)\qquad \left\{\begin{array}{l} \zeta(z)[\zeta(z)+m''-m'][\zeta(z)+2(m''-m')]\ldots \\ \times [\zeta(z)+(p-1)(m''-m')] \equiv \theta_1(z) \equiv 0, \end{array}\right.$$

et ensuite prenons la congruence

$$(\beta_1)\quad \left\{ \begin{array}{l} \Pi[\zeta(z)+bm'+c(m''-m')]\equiv[\theta_1(z)+s_1][\theta_1(z)+2s_1]\ldots \\ \times[\theta_1(z)+(p-1)s_1]\equiv 0, \end{array} \right.$$

$\Pi$ représentant le produit des différents facteurs que l'on obtient en remplaçant $b$ et $c$ par $1, 2, 3, \ldots, p-1$.

Nous pouvons opérer sur les congruences $(\alpha_1)$ et $(\beta_1)$ comme nous avons opéré précédemment sur les congruences $(\alpha')$ et $(\beta')$ et nous arriverons encore aux congruences (A) et (B) qui satisferont aux mêmes conditions.

Ainsi, quels que soient $z_1$ et $\alpha$, on peut former les congruences (A) et (B) qui sont telles que les $p^k$ racines de $(c)$ satisfont à (A) et que $z_1$ et $\alpha$ satisfont à (B); par conséquent la substitution

$$(\gamma)\qquad \left[z, z+a\left(h^{p^{\nu-1}}z^{p^{\nu-1}}+h^{p^{\nu-2}}z^{p^{\nu-2}}+\ldots+hz\right)\right]$$

ne permute pas les $p^k$ variables dont les indices satisfont à $(c)$.

Reste à déterminer $a$ de manière que cette subtitution change $x_{z_1}$ en $x_\alpha$; or il faudra pour cela que l'on ait

$$(k)\qquad z_1+a\left(h^{p^{\nu-1}}z_1^{p^{\nu-1}}+\ldots+h^p z_1^p+hz_1\right)\equiv\alpha.$$

D'ailleurs $z_1$ et $\alpha$ satisfaisant à la congruence (B), on a

$$h^{p^{\nu-1}}z_1^{p^{\nu-1}}+\ldots+h^p z_1^p+hz_1\equiv r,\quad h^{p^{\nu-1}}\alpha^{p^{\nu-1}}+\ldots+h^p\alpha^p+h\alpha\equiv s,$$

$r$ et $s$ étant des nombres entiers égaux ou inégaux, mais différents de zéro; la congruence $(k)$ donnera donc

$$a\equiv\frac{\alpha-z_1}{r}.$$

Il faut toutefois s'assurer qu'en prenant cette valeur pour $a$, l'expression $(\gamma)$ représente bien une substitution, et qu'ainsi l'on n'a pas

$$h^{p^{\nu-1}}a^{p^{\nu-1}}+\ldots+h^p a^p+ha\equiv-1;$$

or, on a

$$h^{p^{\nu-1}} a^{p^{\nu-1}} + \ldots + h^p a^p + ha$$

$$= \frac{h^{p^{\nu-1}}\left(\alpha^{p^{\nu-1}} - z_1^{p^{\nu-1}}\right) + \ldots + h^p\left(\alpha^p - z_1^p\right) + h(\alpha - z_1)}{r} = \frac{s}{r} - 1,$$

quantité différente de $-1$, puisque $s$ est différent de zéro.

Il est donc démontré que la fraction $\Psi$, qui est invariable par toutes les substitutions $(\gamma)$, est transitive par rapport aux $p^\nu - p^k$ variables dont les indices ne satisfont pas à la congruence $(c)$.

Toute substitution dérivée des substitutions $(\gamma)$ est de la forme

$$(l) \qquad \left(z, z + \mu_{\nu-1} z^{p^{\nu-1}} + \mu_{\nu-2} z^{p^{\nu-2}} + \ldots + \mu z\right);$$

et le plus grand commun diviseur de $\mu_{\nu-1} z^{p^{\nu-1}} + \ldots + \mu z$ et de $z^{p^\nu} - z$ est de la même forme que le premier de ces deux polynômes; donc toute substitution dérivée des substitutions $(\gamma)$ s'effectue sur $p^\nu - p^\varepsilon$ variables.

Cela posé, formons les congruences :

$$[0] \qquad z \equiv 0,$$

$$[1] \qquad z(z+a)(z+2a)\ldots(z+\overline{p-1}\,a) \equiv z^p - a^{p-1}z \equiv 0,$$

. . . . . . . . . . . . . . . . . . . . . . . . . . . .

$$z^{p^{\nu-3}} + \ldots + \rho_1 z^p + \rho_0 z \equiv 0,$$

$$[\nu-2]\left\{\begin{aligned} &\left(z^{p^{\nu-3}} + \ldots + \rho_1 z^p + \rho_0 z\right)\left(z^{p^{\nu-3}} + \ldots + \rho_0 z + l\right)\ldots \\ &\times\left(z^{p^{\nu-3}} + \ldots + (p-1)l\right) \equiv z^{p^{\nu-2}} + \sigma_{\nu-3} z^{p^{\nu-3}} + \ldots + \sigma z \equiv 0,\end{aligned}\right.$$

$$[\nu-1]\left\{\begin{aligned} &\left(z^{p^{\nu-2}} + \ldots + \sigma_1 z^p + \sigma_0 z\right)\left(z^{p^{\nu-2}} + \ldots + \sigma_0 z + m\right)\ldots \\ &\times\left(z^{p^{\nu-2}} + \ldots + \sigma_0 z + (p-1)m\right) \\ &\equiv z^{p^{\nu-1}} + \tau_{\nu-2} z^{p^{\nu-2}} + \ldots + \tau_0 z \equiv 0,\end{aligned}\right.$$

dont les premiers membres sont des diviseurs de $z^{p^\nu} - z$, et qui sont telles que chacune contient les racines de la précédente.

Nous voyons que la fonction $\Psi$ est transitive par rapport aux $p^\nu - p^{\nu-1}$ variables dont les indices ne satisfont pas à la congruence $[\nu - 1]$, puis transitive par rapport aux $p^\nu - p^{\nu-2}$ variables dont les indices ne satisfont pas à la congruence $[\nu - 2]$, etc., enfin transitive par rapport aux $p^\nu - 1$ variables autres que $x_0$; d'où l'on déduit facilement que le nombre des valeurs de $\Psi$ est

$$\frac{1.2.3\ldots(p^\nu - 1)}{(p^\nu - p^{\nu-1})(p^\nu - p^{\nu-2})\ldots(p^\nu - p)(p^\nu - 1)},$$

et par suite toutes les subtitutions

$$\left(z, \lambda_{\nu-1} z^{p^{\nu-1}} + \lambda_{\nu-2} z^{p^{\nu-2}} + \ldots \lambda_0 z\right)$$

sont des dérivées des substitutions

$$(\gamma) \qquad \left[z, z + a(h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h^p z^p + hz)\right].$$

Si dans l'expression $(\gamma)$ on change $h$ en $he$, $e$ étant un nombre entier, le polynôme $h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + hz$ est seulement multiplié par $e$; donc si on donne une valeur $\eta$ à $h$, on pourra se dispenser de donner à $h$ les valeurs $2\eta$, $3\eta$,..., $(p-1)\eta$. D'après cela, pour avoir toutes les substitutions $(\gamma)$, on donnera à $h$ $\frac{p^\nu - 1}{p-1}$ valeurs, puis on donnera à la lettre $a$ toutes les valeurs autres que zéro et que celles qui satisfont à

$$h^{p^{\nu-1}} a^{p^{\nu-1}} + h^{p^{\nu-2}} a^{p^{\nu-2}} + \ldots + ha \equiv -1;$$

donc pour chaque valeur de $h$, on a $p^\nu - p^{\nu-1} - 1$ valeurs de $a$, et le nombre des substitutions $(\gamma)$ est $\frac{(p^\nu - 1)(p^\nu - p^{\nu-1} - 1)}{p-1}$.

Enfin nous terminerons cet article en faisant remarquer que la substitution

$$\left(z, z + a(h^{p^{\nu-1}} z^{p^{\nu-1}} + \ldots + h^p z^p + hz) + b\right)$$

est semblable aux substitutions $(\gamma)$, si $\frac{b}{a}$ est racine de $z^p \equiv z$, et que, dans le cas contraire, la substitution s'effectue sur toutes les variables.

*Des fonctions de $p^{\eta\tau}$ variables qui ne sont pas changées par les substitutions* $\left(z, Az^{p^{\eta(\tau-1)}} + Bz^{p^{\eta(\tau-2)}} + \ldots + Hz + L\right)$.

Tout ce que nous avons établi pour les fonctions de $p^\nu$ quantités qui ne sont pas changées par les substitutions

$$\left(z, Az^{p^{\nu-1}} + Bz^{p^{\nu-2}} + \ldots + Hz + L\right),$$

peut être étendu par des raisonnements tout semblables, aux fonctions de $p^{\eta\tau}$ quantités qui sont invariables par les substitutions

$$(\eta) \qquad \left(z, Az^{p^{\eta(\tau-1)}} + Bz^{p^{\eta(\tau-2)}} + \ldots + Iz^{p^{\eta}} + Hz + L\right).$$

Désignons par $0, a_1, a_2, \ldots, a_{p^\eta-1}$ les racines de la congruence

$$z^{p^\eta} - z \equiv 0,$$

dont le premier membre est un diviseur de $z^{p^{\eta\tau}} - z$, nous aurons la congruence

$$\begin{aligned} h\left(z^{p^{\eta\tau}} - z\right) \equiv & \left(h^{p^{\eta(\tau-1)}} z^{p^{\eta(\tau-1)}} + h^{p^{\eta(\tau-2)}} z^{p^{\eta(\tau-2)}} + \ldots + h^{p^\eta} z^{p^\eta} + hz\right) \\ & \times \left(h^{p^{\eta(\tau-1)}} z^{p^{\eta(\tau-1)}} + \ldots + h^{p^\eta} z^{p^\eta} + hz + a_1\right) \\ & \times \left(h^{p^{\eta(\tau-1)}} z^{p^{\eta(\tau-1)}} + \ldots + hz + a_2\right) \ldots \\ & \times \left(h^{p^{\eta(\tau-1)}} z^{p^{\eta(\tau-1)}} + \ldots + hz + a_{p^\eta-1}\right). \end{aligned}$$

Soient $\alpha^{1,1}, \alpha^{1,2}, \alpha^{1,3}, \ldots, \alpha^{1,p^{\eta(\tau-1)}}$ les racines de $z^{p^{\eta\tau}} \equiv z$ dues au premier facteur; $\alpha^{2,1}, \alpha^{2,2}, \alpha^{2,3}, \ldots, \alpha^{2,p^{\eta(\tau-1)}}$ les racines de $z^{p^{\eta\tau}} \equiv z$ dues au second; $\alpha^{3,1}, \alpha^{3,2}, \ldots, \alpha^{3,p^{\eta(\tau-1)}}$ celles qui sont dues au troi-

sième, et ainsi de suite. Prenons la fonction

$$x_{\alpha^{1,1}} x_{\alpha^{1,2}} \ldots x_{\alpha^{1,p^{\eta(\tau-1)}}} + x_{\alpha^{2,1}} x_{\alpha^{2,2}} \ldots x_{\alpha^{2,p^{\eta(\tau-1)}}}$$
$$+ x_{\alpha^{3,1}} x_{\alpha^{3,2}} \ldots x_{\alpha^{3,p^{\eta(\tau-1)}}} + \ldots;$$

soit $\omega$ une racine primitive de $z^{p^{\eta\tau}} \equiv z$; faisons sur cette fonction les $\frac{p^{\eta\tau} - p^\eta}{p^\eta - 1}$ premières puissances de $(z, \omega z)$, et formons une fonction symétrique des $\frac{p^{\eta\tau} - 1}{p^\eta - 1}$ fonctions ainsi obtenues; nous aurons ainsi une fonction invariable par les substitutions $(\eta)$.

Désignons par o, $b_1, b_2, \ldots b_{p^{\eta(\tau-1)}}$ les racines de la congruence

$$z^{p^{\eta(\tau-1)}} + z^{p^{\eta(\tau-2)}} + \ldots + z^{p^\eta} + z \equiv 0,$$

nous aurons la congruence identique

$$\lambda\left(z^{p^{\eta\tau}} - z\right) \equiv \left(\lambda^{p^\eta} z^{p^\eta} - \lambda z\right)\left(\lambda^{p^\eta} z^{p^\eta} - \lambda z - b_1\right)\left(\lambda^{p^\eta} z^{p^\eta} - \lambda z - b_2\right)\ldots$$
$$\times \left(\lambda^{p^\eta} z^{p^\eta} - \lambda z - b_{p^{\eta(\tau-1)}-1}\right).$$

Soient $\alpha_1, \alpha_2, \ldots, \alpha_{p^\eta}$ les racines de $z^{p^{\eta\tau}} \equiv z$ dues au premier facteur, soient $\beta_1, \beta_2, \ldots, \beta_{p^\eta}$ les racines qui sont dues au second, $\gamma_1, \gamma_2, \ldots, \gamma_{p^\eta}$ celles qui sont dues au troisième et ainsi de suite. Faisons sur la fonction

$$\varphi = x_{\alpha_1} x_{\alpha_2} \ldots x_{\alpha_{p^\eta}} + x_{\beta_1} x_{\beta_2} \ldots x_{\beta_{p^\eta}} + x_{\gamma_1} x_{\gamma_2} \ldots x_{\gamma_{p^\eta}} + \ldots$$

les $\frac{p^{\eta\tau} - p^\eta}{p^\eta - 1}$ premières puissances de $(z, \omega z)$, $\omega$ étant racine primitive de $z^{p^{\eta\tau}} = z$, nous aurons ainsi $\frac{p^{\eta\tau} - p^\eta}{p^\eta - 1}$ fonctions; ajoutons-y la fonction $\varphi$; enfin formons une fonction symétrique de ces fonctions, et nous aurons encore une fonction invariable par les substitutions $(\eta)$.

Le nombre des substitutions $(\eta)$ est égal à

$$p^{\eta\tau}(p^{\eta\tau} - 1)(p^{\eta\tau} - p^\eta)(p^{\eta\tau} - p^{2\eta}) \ldots (p^{\eta\tau} - p^{\eta(\tau-1)}),$$

et par conséquent le nombre des valeurs de la fonction de $p^{\eta\tau}$ quantités qui n'est pas changée par ces substitutions est

$$\frac{1.2.3\ldots(p^{\eta\tau}-1)}{(p^{\eta\tau}-p^{\eta(\tau-1)})(p^{\eta\tau}-p^{\eta(\tau-2)})\ldots(p^{\eta\tau}-p^{\eta})(p^{\eta\tau}-1)}.$$

Si on désigne par $\Omega$ une racine d'une congruence du degré $\tau$, dont les coefficients sont racines de $z^{p^\eta}\equiv z$, et dont le premier membre n'a aucun facteur commun avec $z^{p^\eta}-z$, toutes les racines de $z^{p^{\eta\tau}}\equiv z$, lesquelles sont les indices de nos $p^{\eta\tau}$ variables, sont renfermées dans l'expression

$$(\mu)\qquad A_0+A_1\Omega+A_2\Omega^2+\ldots+A_{\tau-1}\Omega^{\tau-1},$$

$A_0, A_1, A_2,\ldots, A_{\tau-1}$ étant racines de la congruence $z^{p^\eta}\equiv z$.

Si on désigne ensuite par $\nu_0, \nu_1,\ldots, \nu_{\tau-1}$ les valeurs en lesquelles les indices $1, \Omega, \Omega^2,\ldots, \Omega^{\tau-1}$ sont changés par la substitution

$$(m)\qquad \left(z,\ \lambda_{\tau-1}z^{p^{\eta(\tau-1)}}+\lambda_{\tau-2}z^{p^{\eta(\tau-2)}}+\ldots\lambda_1 z^{p^\eta}+\lambda_0 z\right),$$

nous aurons les congruences

$$\lambda_{\tau-1}+\lambda_{\tau-2}+\lambda_{\tau-3}+\ldots+\lambda_1+\lambda_0\equiv\nu_0,$$

$$\Omega^{p^{\eta(\tau-1)}}\lambda_{\tau-1}+\Omega^{p^{\eta(\tau-2)}}\lambda_{\tau-2}+\Omega^{p^{\eta(\tau-3)}}\lambda_{\tau-3}+\ldots+\Omega^{p^\eta}\lambda_1+\Omega\lambda_0\equiv\nu_1,$$

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

$$\Omega^{(\tau-1)p^{\eta(\tau-1)}}\lambda_{\tau-1}+\Omega^{(\tau-1)p^{\eta(\tau-2)}}\lambda_{\tau-2}+\ldots+\Omega^{\tau-1}\lambda_0\equiv\nu_{\tau-1},$$

et l'indice en lequel sera changé l'indice $(\mu)$ sera donné par l'expression

$$A_0\nu_0+A_1\nu_1+\ldots+A_{\tau-1}\nu_{\tau-1}.$$

Ainsi pour que l'expression $(m)$ représente une substitution, il faut que $\nu_0, \nu_1,\ldots, \nu_{\tau-1}$ soient tels, que l'on n'ait pas

$$\nu_k=\alpha_0\nu_0+\alpha_1\nu_1+\ldots+\alpha_{k-1}\nu_{k-1},$$

$\alpha_0, \alpha_1,\ldots, \alpha_{k-1}$ étant des racines de la congruence $z^{p^\eta}\equiv z$.

Soient $\Omega_0, \Omega_1, \ldots, \Omega_{\tau-1}$ $\tau$ racines de la congruence $z^{p^{\eta\tau}} \equiv z$ telles, que l'on n'ait pas $\Omega_k \equiv \alpha_0 \Omega_0 + \alpha_1 \Omega_1 + \ldots + \alpha_{k-1} \Omega_{k-1}$, $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}$ étant racines de $z^{p^\eta} \equiv z$; la fonction de $p^{\eta\tau}$ variables qui n'est pas changée par toutes les substitutions $(\eta)$ est transitive par rapport aux $p^{\eta\tau} - 1$ variables autres que $x_0$, puis transitive par rapport aux $p^{\eta\tau} - p^\eta$ variables qui ne sont pas de la forme $x_{\alpha_0 \Omega_0}$, puis transitive par rapport aux $p^{\eta\tau} - p^{2\eta}$ variables qui ne sont pas de la forme $x_{\alpha_0 \Omega_0 + \alpha_1 \Omega_1}$, et ainsi de suite.

Toutes les substitutions $(\eta)$ sont des dérivées des substitutions

$$\left| z,\ z + a\left(h^{p^{\eta(\tau-1)}} z^{p^{\eta(\tau-1)}} + h^{p^{\eta(\tau-2)}} z^{p^{\eta(\tau-2)}} + \ldots + h^{p^\eta} z^{p^\eta} + hz\right)\right|$$

qui s'effectuent sur $p^{\eta\tau} - p^{\eta(\tau-1)}$ variables.

---

## CHAPITRE IV.

### DES FONCTIONS TRANSITIVES D'UN NOMBRE PREMIER DE QUANTITÉS.

Nous commencerons l'étude de ces fonctions par un théorème qui est fondamental, et que nous avons reconnu aussitôt que nous nous sommes occupé du sujet de ce Mémoire, mais dont la démonstration, quoique assez simple, nous a longtemps échappé. Cette proposition est celle-ci :

Théorème. — *Une fonction transitive d'un nombre premier de quantités est nécessairement invariable par une certaine substitution circulaire effectuée sur toutes les quantités.*

Pour démontrer ce théorème, nous établirons d'abord ce lemme :

Soient $a, b, c, \ldots, k, l$, les $p$ quantités, et supposons que K soit le nombre des substitutions effectuées sur $p - r$ lettres qui laissent $l$ immobile, et qui laissent la fonction F considérée invariable; F est invariable par $\frac{\mathrm{K}p}{r}$ substitutions effectuées sur $p - r$ lettres.

En effet, considérons $p - 1$ lettres quelconques de la fonction tran-

sitive F; il y a sur ces $p-1$ lettres K substitutions de $p-r$ lettres, qui laissent F invariable. Faisons la somme des substitutions de $p-r$ lettres que l'on a pour chaque arrangement de $p-1$ lettres, nous aurons ainsi $Kp$ substitutions de $p-r$ lettres; mais il est aisé de voir que chaque substitution se trouve répétée $r$ fois, de sorte qu'il n'y a que $\frac{Kp}{r}$ substitutions de $p-r$ lettres qui ne changent pas la fonction transitive F. En effet, si en considérant les $p-1$ lettres $a, b,\ldots, e, f,\ldots, i, k$, on a une substitution faite sur les $p-r$ lettres $a, b,\ldots, e$, on a pareillement cette substitution de $p-r$ lettres en considérant les $p-1$ lettres $a, b,\ldots, e, f,\ldots, i, l$, et en général on a cette substitution dans tous les groupes de $p-1$ lettres, que l'on obtient en prenant les $p-r$ lettres $a, b,\ldots, e$ avec $r-1$ des lettres restantes. Donc dans les $Kp$ substitutions ci-dessus obtenues, la substitution que nous venons de considérer sur les $p-r$ lettres $a, b,\ldots, e$ se trouve répétée autant de fois que l'on peut combiner $r$ quantités $r-1$ à $r-1$, c'est-à-dire $r$ fois, et notre lemme est démontré.

Démontrons ensuite cet autre principe : S'il existe une substitution S de $p$ lettres non circulaire qui laisse invariable la fonction F, le nombre des substitutions semblables à S et qui laissent F invariable, est divisible par $p$.

Soit $\beta$ le nombre des lettres d'un certain cycle de S; prenons la puissance $\beta^{\text{ième}}$ de cette substitution, nous aurons pour cette puissance une certaine substitution A.

A étant ainsi défini, soit $g$ une des lettres qui ne se trouvent pas dans A, et désignons par

$$(\alpha)\qquad A,\ A',\ A'',\ldots,\ A^{(\nu-1)},$$

les $\nu$ substitutions semblables à A, et qui ne contiennent pas $g$.

Considérons $p-1$ lettres de la fonction F, qui ne comprennent pas la lettre $h$ autre que $g$; il y aura sur ces $p-1$ lettres $\nu$ substitutions

$$(\beta)\qquad A_1,\ A'_1,\ A''_1,\ldots,\ A_1^{(\nu-1)}$$

semblables à A, et qui ne différeront des substitutions $(\alpha)$ que par la

manière de désigner les variables; ainsi on passera des substitutions $(\alpha)$ aux substitutions $(\beta)$ en faisant sur les variables une même substitution.

Considérons de même les $p-1$ lettres autres que $i$, $i$ étant différent de $g$ et de $h$, et ainsi de suite. Nous aurons en définitive les $\nu p$ substitutions

$$(\gamma)\quad \left\{\begin{array}{lllll} A, & A', & A'', \ldots, & A^{(\nu-1)}, \\ A_1, & A'_1, & A''_1, \ldots, & A_1^{(\nu-1)}, \\ \ldots & \ldots & \ldots & \ldots \\ A_{p-1}, & A'_{p-1}, & A''_{p-1}, \ldots, & A_{p-1}^{(\nu-1)}, \end{array}\right.$$

parmi lesquelles il n'y en a que $\frac{\nu}{r}p$ qui soient distinctes, $p-r$ étant le nombre des lettres permutées par A. On passera des substitutions d'une ligne horizontale du groupe $(\gamma)$ à celles d'une autre ligne en faisant une même substitution sur les variables des substitutions de la première de ces deux lignes.

Supposons maintenant que $S, S^{(1)}, S^{(2)}, \ldots, S^{(i-1)}$ soient toutes les substitutions semblables à S qui ont A pour puissance $\beta^{\text{ième}}$, et qui laissent F invariable. Désignons ensuite par $R^{(0)}, R^{(1)}, \ldots, R^{(s-1)}$ toutes les substitutions semblables à S qui ont A' pour puissance $\beta^{\text{ième}}$, etc., enfin par $L^{(0)}, L^{(1)}, \ldots, L^{(t-1)}$ toutes les substitutions semblables à S qui ont $A^{(\nu-1)}$ pour puissance $\beta^{\text{ième}}$. Nous aurons ainsi les $\mu$ substitutions

$$(\delta)\quad S, S^{(1)}, S^{(2)}, \ldots, S^{(i-1)}, R^{(0)}, R^{(1)}, \ldots, R^{(s-1)}, \ldots, L^{(0)}, L^{(1)}, \ldots, L^{(t-1)},$$

qui sont toutes différentes; par exemple les substitutions $R^{(0)}, R^{(1)}, \ldots, R^{(s-1)}$ sont différentes entre elles, et elles sont différentes de $S, S^{(1)}, \ldots, S^{(i-1)}$, puisqu'elles ont une puissance $\beta^{\text{ième}}$ différente.

Nous observons alors que tout ce qui a lieu pour les substitutions

$$A, A', A'', \ldots, A^{(\nu-1)},$$

a lieu identiquement, et pour les substitutions

$$A_1, A'_1, A''_1, \ldots, A_1^{(\nu-1)},$$

et pour les substitutions

$$A_2,\ A'_2,\ A''_2,\ldots,\ A_2^{(\nu-1)},$$

etc. Ainsi il y a $\mu$ substitutions

$$(\varepsilon)\quad S_1^{(0)},\ S_1^{(1)},\ S_1^{(2)},\ldots,\ S_1^{(i-1)},\ R_1^{(0)},\ R_1^{(1)},\ldots,\ R_1^{(s-1)},\ldots,\ L_1^{(0)},\ L_1^{(1)},\ldots,\ L_1^{(t-1)},$$

différentes entre elles, et qui ont pour puissance $\beta^{ième}$ les $i$ premières $A_1$, les $s$ suivantes $A'_1$, etc , les $t$ dernières $A_1^{(\nu-1)}$. Il y a $\mu$ substitutions

$$(\zeta)\quad S_2^{(0)},\ S_2^{(1)},\ S_2^{(2)},\ldots,\ S_2^{(i-1)},\ R_2^{(0)},\ R_2^{(1)},\ldots,\ R_2^{(s-1)},\ldots,\ L_2^{(0)},\ L_2^{(1)},\ldots,\ L_2^{(t-1)},$$

différentes entre elles, et qui ont pour puissance $\beta^{ième}$ les $i$ premières $A_2$, les $s$ suivantes $A'_2$, etc., les $t$ dernières $A_2^{(\nu-1)}$. Et ainsi de suite.

On passe des substitutions ($\delta$) aux substitutions ($\varepsilon$), puis aux substitutions ($\zeta$), etc., en faisant sur les variables les substitutions au moyen desquelles on passe de la première ligne horizontale des substitutions ($\gamma$) à la seconde, puis à la troisième, etc.

Actuellement les substitutions ($\gamma$) étant identiques $r$ à $r$, les $\mu p$ substitutions ($\delta$), ($\varepsilon$), ($\zeta$), etc., sont aussi identiques $r$ à $r$; le nombre de ces substitutions qui sont distinctes est donc $\frac{\mu p}{r}$, et puisque $r$ est $< p$, ce nombre est divisible par $p$.

D'ailleurs il n'y a pas d'autres substitutions que les substitutions ($\delta$), ($\varepsilon$), ($\zeta$), etc., qui soient semblables à S et qui laissent F invariable. Notre principe est donc démontré.

Cela posé, considérons toutes les substitutions qui ne comprennent pas une certaine lettre $g$, et qui laissent F invariable, et soient $K_1$ le nombre de celles qui s'effectuent sur $p - r_1$ lettres, $K_2$ le nombre de celles qui s'effectuent sur $p - r_2$ lettres, etc. Désignons enfin par $rp$ le nombre des substitutions qui laissent F invariable; le nombre des substitutions qui s'effectuent sur toutes les lettres, est

$$rp - p\left(\frac{K_1}{r_1} + \frac{K_2}{r_2} + \ldots + \frac{K_i}{r_i}\right) - 1;$$

c'est donc un nombre non divisible par $p$; car $\frac{K_1}{r_1}$, $\frac{K_2}{r_2}$, etc., sont des nombres entiers. Il est donc nécessaire que quelques-unes de ces substitutions soient circulaires.

Corollaire. — *Le nombre des substitutions circulaires distinctes de $p$ lettres qui laissent invariable une fonction transitive de $p$ lettres est de la forme $\alpha p + 1$.*

En effet, si l'on désigne par $x$ le nombre des substitutions circulaires distinctes de $p$ lettres, et par $py$ le nombre de toutes les substitutions non circulaires de $p$ lettres, on a

$$(p-1)x + py = rp - p\left(\frac{K_1}{r_1} + \frac{K_2}{r_2} + \ldots + \frac{Ki}{r_i}\right) - 1,$$

d'où

$$x = \alpha p + 1.$$

Le raisonnement précédent conduit également à ce théorème :

*Une fonction transitive dont le nombre des lettres est une puissance d'un nombre premier, est invariable par quelque substitution régulière effectuée sur toutes ses lettres.*

D'après cela, étant donnée une fonction transitive d'un nombre premier $p$ de quantités, nous désignerons ces $p$ quantités par $x_0$, $x_1$, $x_2, \ldots, x_{p-1}$, et supposerons que cette fonction est invariable par la substitution

$$(x_0 x_1 x_2 \ldots x_{p-1})$$

ou $(z, z+1)$ en convenant que $x_a = x_e$, si l'on a $a \equiv e \pmod{p}$.

Il est facile de démontrer que *si une fonction transitive de $p$ quantités n'est invariable que par des substitutions effectuées sur $p$ et sur $p-1$ quantités, toutes ces substitutions sont données par l'expression*

$$(\alpha) \qquad (z, a^u z + b),$$

*$u$ étant un diviseur de $p-1$.*

On voit d'abord que si l'on désigne par $\alpha p$ le nombre total des

substitutions, le nombre des substitutions de $p$ quantités est $\alpha p - 1 - p(\alpha - 1) = p - 1$, de sorte qu'elles sont toutes comprises dans l'expression $(z, z + m)$.

Soit $(z, \theta_r z)$ une quelconque des substitutions effectuées sur $x_1$, $x_2, \ldots, x_{p-1}$; $[\theta_r z, \theta_r(z + m)]$ est une substitution semblable à $(z, z + m)$, puisqu'on l'obtient en faisant sur les variables de $(z, z + m)$ la substitution $(z, \theta_r z)$; désignons par $\theta'_r z$ la fonction inverse de $\theta_r z$, cette substitution pourra s'écrire $[z, \theta_r(\theta'_r z + m)]$; or cette substitution laisse la fonction considérée invariable, elle est donc identique à une des substitutions $(z, z + n)$ et on aura

$$\theta_r(\theta'_r z + m) \equiv z + n \pmod{p},$$

d'où

$$\theta'_r(z + n) \equiv \theta'_r z + m.$$

De cette congruence, on tire

$$\theta'_r(z + 2n) \equiv \theta'_r(z + n) + m \equiv \theta'_r z + 2m,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\theta'_r(z + kn) \equiv \theta'_r z + km.$$

Faisons $z = 0$, nous aurons, $k$ étant quelconque,

$$\theta'_r(kn) \equiv \theta'_r 0 + km;$$

$\theta'_r 0$ est nul; on a donc, en remplaçant $kn$ par $z$,

$$\theta'_r z \equiv \frac{m}{n} z,$$

et par conséquent toutes les substitutions qui laissent la fonction considérée invariable, sont comprises dans la formule $(\alpha)$.

On voit aussi par cette démonstration que si une fonction transitive de $p$ quantités n'est invariable que par une seule substitution circulaire de $p$ quantités, toutes les substitutions qui la laissent invariable sont les substitutions $(\alpha)$.

Or le nombre des substitutions circulaires qui laissent une fonction transitive de $p$ lettres invariable est de la forme $\alpha p + 1$; donc si une fonction transitive de $p$ quantités est invariable par d'autres substitutions que les substitutions ($\alpha$), elle est invariable par au moins $p+1$ substitutions circulaires.

Théorème. — *Une fonction transitive F de p quantités est invariable par toutes les substitutions* $(z, a^u z + b)$, *a et b étant quelconques et u un certain diviseur de* $p-1$ *plus petit que* $p-1$, *et même plus petit que* $\frac{p-1}{2}$ *si p est de la forme* $4n-1$. *Le nombre des substitutions circulaires de p quantités qui laissent cette fonction invariable est au moins égal à* $\frac{ru}{p-1}$, *r étant le nombre des substitutions qui, effectuées sur* $x_1, x_2, \ldots, x_{p-1}$, *laissent cette fonction invariable.*

La fonction F est supposée invariable par la substitution $(z, z+1)$ et soient ensuite

$$(1) \qquad (z, z), \quad (z, \theta_1 z), \ (z, \theta_2 z), \ldots, \quad (z, \theta_{r-1} z)$$

les substitutions qui ne permutent que $x_1, x_2, \ldots, x_{p-1}$ et qui laissent la fonction F invariable.

Les substitutions $[\theta_s z, \theta_s (z+m)]$ ou $[z, \theta_s(\theta'_s z + m)]$ sont des substitutions circulaires, qui sont les puissances de $[z, \theta_s(\theta'_s z + 1)]$. Or, le nombre total des substitutions qui laissent F invariable est $rp$; donc, en faisant dans l'expression $[z, \theta_s(\theta'_s z + m)] s = 0, 1, 2, \ldots, r-1$, on n'obtiendra pas toutes des substitutions circulaires différentes, puisque, si elles étaient toutes différentes, on aurait $r(p-1)$ substitutions circulaires de $p$ variables, et par conséquent le nombre de toutes les substitutions qui ont moins de $p$ variables serait au plus égal à $r$, ce qui est absurde; donc il y aura nécessairement deux substitutions telles que $[z, \theta_s(\theta'_s z + m)]$ et $[z, \theta_v(\theta'_v z + n)]$ qui seront identiques: ce qui donnera

$$\theta_s(\theta'_s z + m) = \theta_v(\theta'_v z + n) \quad (\text{mod. } p.).$$

Changeons $z$ en $\theta_v z$, et nous aurons

$$\theta_s(\theta'_s \theta_v z + m) \equiv \theta_v(z + n),$$

$$\theta'_s \theta_v z + m \equiv \theta'_s \theta_v (z + n).$$

Posons

(2) $$\theta'_s \theta_v z \equiv \theta_t z,$$

et nous obtiendrons

$$\theta_t(z + n) \equiv \theta_t z + m,$$

ce qui donne

(3) $$\theta_t z \equiv cz,$$

et il est prouvé que les substitutions (1) contiennent toutes les substitutions $(z, a^u z)$, $u$ étant un diviseur de $p - 1$.

Démontrons ensuite que si $p$ est de la forme $4n - 1$, $u$ est plus petit que $\frac{p-1}{2}$, si la fonction est invariable par d'autres substitutions que les substitutions $\left[z, (\pm 1)^{\frac{p-1}{2}} z + b\right]$.

En effet, supposons cette fonction de $p$ quantités invariable par les substitutions $(z, \pm z + b)$, et par d'autres qui ne soient pas de la forme $(z, az + b)$. Multiplions cette fonction par la fonction des mêmes quantités qui a deux valeurs, laquelle est changée par la substitution $(z, -z)$, et nous obtiendrons une fonction transitive de $p$ quantités qui ne serait invariable par aucune des substitutions $(z, az)$, ce qui est impossible.

On voit en particulier que si $\frac{p-1}{2}$ *est un nombre premier, une fonction transitive de p quantités qui n'est pas la fonction invariable par les seules substitutions* $(z, \pm z + b)$, *est invariable par toutes les substitutions* $(z, a^2 z + b)$.

Pour achever la démonstration de notre théorème, supposons qu'il y ait $e$ des expressions $\theta(\theta' z + m)$, qui puissent servir à représenter une

même substitution circulaire, de sorte que l'on ait

$$(4)\quad \begin{cases} \theta_s(\theta'_s z+n)\equiv\theta_{s_1}(\theta'_{s_1}z+n_1)\equiv\theta_{s_2}(\theta'_{s_2}z+n_2)\equiv\ldots \\ \equiv\theta_{s_{e-1}}\left(\theta'_{s_{e-1}}z+n_{e-1}\right); \end{cases}$$

de la première de ces congruences on tire, en changeant $z$ en $\theta'_k z$ inverse de $\theta_k z$,

$$\theta_s(\theta'_s\,\theta'_k z+n)\equiv\theta_{s_1}(\theta'_{s_1}\theta'_k z+n_1),$$

et

$$\theta_k\theta_s(\theta'_s\,\theta'_k z+n)\equiv\theta_k\theta_{s_1}(\theta'_{s_1}\theta'_k z+n_1);$$

donc on aura

$$\theta_k\theta_s(\theta'_s\,\theta'_k z+n)\equiv\theta_k\theta_{s_1}(\theta'_{s_1}\theta'_k z+n_1)\equiv\ldots\equiv\theta_k\theta_{s_{e-1}}\left(\theta'_{s_{e-1}}\theta'_k z+n_{e-1}\right);$$

$\theta'_s\,\theta'_k\,z$ est l'inverse de $\theta_k\,\theta_s z$; donc toutes les expressions $\theta\,(\theta' z+m)$ sont égales $e$ à $e$. D'après les congruences (2) et (3), on aura

$$\theta'_s\,\theta_{s_1}z\equiv c_1 z,\quad \theta'_s\,\theta_{s_2}z\equiv c_2 z,\ldots,\quad \theta'_s\,\theta_{s_{e-1}}z\equiv c_{e-1}z,$$

et par conséquent il y a $e$ substitutions de la forme $(z, cz)$, qui laissent la fonction invariable, et il n'y en a pas davantage; car s'il y en avait plus, on pourrait poser $\theta'_s\,\theta_g z\equiv dz$, $\theta_g$ étant différent de $\theta_{s_1}, \theta_{s_2},\ldots, \theta_{s_{e-1}}$, et on aurait à ajouter aux $e$ termes (4) congrus entre eux le terme $\theta_g(\theta'_g z+q)$; donc ces $e$ substitutions ne sont pas autres que les substitutions $(z, a^u z)$, et on a $e=\frac{p-1}{u}$.

Les $r$ expressions $\theta_s(\theta'_s z+1)$ peuvent donc être groupées $e$ à $e$, de manière à être identiques ou puissances l'une de l'autre; donc le nombre des substitutions circulaires distinctes renfermées dans l'expression $[z, \theta(\theta' z+1)]$ est $\frac{r}{e}$ ou $\frac{ru}{p-1}$. Comme toutefois nous n'avons pas démontré que toutes les substitutions circulaires qui laissent la fonction invariable sont de la forme $[z, \theta(\theta' z+m)]$, il faudrait bien se

garder de croire que le nombre de ces substitutions circulaires est égal à $\frac{ru}{p-1}$, mais seulement qu'il est au moins égal à $\frac{ru}{p-1}$.

D'après ce que nous venons de voir, les substitutions (1) qui s'effectuent sur $x_1, x_2, \ldots, x_{p-1}$ peuvent s'écrire

$$(\varepsilon) \qquad (z, a^u z), \quad (z, a^u \theta_1 z), \quad (z, a^u \theta_2 z), \ldots, \quad (z, a^u \theta_{r'-1} z).$$

Si $u$ est impair, en multipliant la fonction invariable par les substitutions $(\varepsilon)$ par la fonction qui a deux valeurs, on aura une fonction qui ne sera invariable que par les substitutions $(z, a^u z)$ pour lesquelles $a$ est résidu quadratique, et comme le nombre des substitutions qui la laissent invariable doit devenir deux fois moindre, ce sont

$$(z, a^{2u} z), \quad (z, a^{2u} \theta_1 z), \quad (z, a^{2u} \theta_2 z), \ldots, \quad (z, a^{2u} \theta_{r'-1} z);$$

on voit donc aussi que les substitutions

$$(z, \theta_1 z), \quad (z, \theta_2 z), \ldots, \quad (z, \theta_{r'-1} z)$$

laissent invariable la fonction qui a deux valeurs.

Supposons une fonction de $p+1$ variables qui ne soit pas changée par toutes les substitutions $\left(z, \frac{Az+B}{Cz+D}\right)$ pour lesquelles $(AD - BC)$ est résidu quadratique, ni par les substitutions (1); $(z, a^2 z)$ figure donc parmi ces dernières substitutions. La substitution $\left\{z, \frac{(-1)^{\frac{p-1}{2}}}{\theta_r \left[\frac{(-1)^{\frac{p-1}{2}}}{z}\right]}\right\}$ laisse cette fonction invariable et ne permute ni $x_0$, ni $x_\infty$; c'est donc une des substitutions (1), et on a

$$\frac{(-1)^{\frac{p-1}{2}}}{\theta_r \left[\frac{(-1)^{\frac{p-1}{2}}}{z}\right]} = \theta_u z,$$

d'où

$$(g) \qquad \theta_u z \theta_v \left[\frac{(-1)^{\frac{p-1}{2}}}{z}\right] \equiv (-1)^{\frac{p-1}{2}}.$$

Il est ensuite aisé de démontrer que si l'on a $\theta_t(z+m) \equiv \theta_g z + n$, quel que soit $t$, et que si toutes les substitutions (1) sont assujetties à la congruence $(g)$, il existe une fonction deux fois transitive de $p+1$ quantités invariable par les substitutions (1) et par les substitutions $\left(z, \frac{Az+B}{Cz+D}\right)$ pour lesquelles AD — BC est résidu quadratique, et si l'on écrit les substitutions (1)

$$(z, a^2 z), \quad (z, a^2\theta_1 z), \quad (z, a^2\theta_2 z), \ldots, \quad (z, a^2\theta_{\varepsilon-1} z),$$

$\varepsilon$ étant égal à $\frac{2r}{p-1}$, toutes les substitutions qui laissent cette fonction invariable sont données par l'expression

$$\left(z, \frac{A\theta_s z + B}{C\theta_s z + D}\right),$$

AD — BC étant résidu quadratique (et $s < \varepsilon$).

Théorème. — *Soit une fonction transitive d'un nombre premier $p$ de lettres, dont toutes les substitutions s'effectuant sur $p$ lettres sont circulaires; si elle est invariable par des substitutions qui changent la fonction qui a deux valeurs, toutes ces substitutions s'effectuent sur $p-1$ lettres.*

Supposons en effet une fonction F de $p$ lettres, dont toutes les substitutions de $p$ lettres soient circulaires, et qui soit invariable par des substitutions qui changent la fonction des mêmes lettres, qui a deux valeurs.

Considérons les substitutions qui ne contiennent pas $x_0$ et qui laissent F invariable. Soient $K_1$ le nombre de ces substitutions effectuées sur $p-r_1$ lettres, $K_2$ le nombre de ces substitutions effectuées sur $p-r_2$ lettres, etc. Le nombre des substitutions de moins de $p$ lettres

qui laissent F invariable est

$$\frac{K_1 p}{r_1} + \frac{K_2 p}{r_2} + \ldots + \frac{K_i p}{r_i} + 1,$$

et l'on a, en désignant par $rp$ le nombre des substitutions qui laissent F invariable,

$$(\alpha) \qquad r = K_1 + K_2 + \ldots + K_i + 1;$$

donc le nombre des substitutions de $p$ lettres qui, par hypothèse, sont toutes circulaires, est

$$rp - \left(\frac{K_1 p}{r_1} + \frac{K_2 p}{r_2} + \ldots + \frac{K_i p}{r_i} + 1\right).$$

Multiplions la fonction F par la fonction des mêmes lettres qui a deux valeurs, nous aurons une fonction transitive F' dont le nombre des valeurs égales est $\frac{r}{2}p$. Considérons encore les substitutions qui ne contiennent pas $x_0$, et qui laissent F' invariable. Soient $K'_1$ le nombre de ces substitutions effectuées sur $p - r_1$ lettres, $K'_2$ le nombre de ces substitutions effectuées sur $p - r_2$ lettres, etc. Le nombre des substitutions de moins de $p$ lettres, qui laissent F' invariable, est

$$\frac{K'_1 p}{r_1} + \frac{K'_2 p}{r_2} + \ldots + \frac{K'_i p}{r_i} + 1,$$

et on a

$$(\beta) \qquad \frac{r}{2} = K'_1 + K'_2 + \ldots + K'_i + 1;$$

quant au nombre des substitutions circulaires de $p$ lettres qui laissent F' invariable, il est

$$\frac{rp}{2} - \left(\frac{K'_1 p}{r_1} + \frac{K'_2 p}{r_2} + \ldots + \frac{K'_i p}{r_i} + 1\right).$$

Or le nombre des substitutions circulaires de $p$ lettres qui laissent les

deux fonctions F et F′ invariables est le même; on a donc

$$rp - p\left(\frac{K_1}{r_1} + \frac{K_2}{r_2} + \ldots + \frac{K_i}{r_i} + \frac{1}{p}\right) = \frac{rp}{2} - p\left(\frac{K'_1}{r_1} + \frac{K'_2}{r_2} + \ldots + \frac{1}{p}\right),$$

d'où

$$\frac{r}{2} = \frac{K_1 - K'_1}{r_1} + \frac{K_2 - K'_2}{r_2} + \ldots + \frac{K_i - K'_i}{r_i}.$$

En retranchant $(\beta)$ de $(\alpha)$, on a d'autre part

$$\frac{r}{2} = (K_1 - K'_1) + (K_2 - K'_2) + \ldots + (K_i - K'_i),$$

et en comparant ces deux dernières égalités, on a

$$r_1 = 1, \quad K_2 = K'_2, \quad K_3 = K'_3 \ldots$$

Nous ferons remarquer à propos de ce théorème ce fait digne d'attention, que nous ne connaissons aucune fonction transitive d'un nombre premier de quantités invariable par d'autres substitutions que $(z, az + b)$ et qui ne soit pas changée par des substitutions qui changent la fonction qui a deux valeurs.

Enfin nous pouvons certifier ce théorème, quoique nous n'en connaissions pas de démonstration rigoureuse : *Une fonction transitive d'un nombre premier de quantités ne peut être invariable par des substitutions qui s'effectuent sur moins de $\frac{p+1}{2}$ de ces quantités.*

Soit $(z, \theta z)$ une substitution des $p - 1$ variables $x_1, x_2, \ldots, x_{p-1}$ pour laquelle on a $\theta(a^u z) = \alpha^u \theta z$, $u$ étant un diviseur de $p - 1$; cette substitution est de la forme

$$(1)\quad \left[\begin{array}{l} z,\ Az^{\lambda + (u-1)\frac{p-1}{u}} + Bz^{\lambda + (u-2)\frac{p-1}{u}} + \ldots + Iz^{\lambda + 2\frac{p-1}{u}} \\ \qquad + Kz^{\lambda + \frac{p-1}{u}} + Lz^{\lambda} \end{array}\right].$$

D'ailleurs les dérivées des substitutions de cette forme sont encore de la même forme; car si l'on a

$$\theta(a^u z) = \alpha^u \theta z, \quad \mu(a^u z) = \beta^u \mu z,$$

on aura

$$\theta\mu(a^{u}z) = \theta(\beta^{u}\mu z) \quad \text{et} \quad \theta\mu(a^{u}z) = \gamma^{u}\theta\mu z.$$

On voit donc que, $\lambda$ étant un nombre variable, les substitutions de la forme (1) jointes aux substitutions $(z, az)$ forment un système de substitutions conjuguées, et la fonction de $p-1$ quantités invariable par ces substitutions est transitive, puisqu'elle est invariable par toutes les substitutions $(z, az)$.

Actuellement considérons une fonction transitive de $p$ quantités, invariable par toutes les substitutions $(z, a^{u}z+b)$, et soient

$$(2) \qquad (z, z), \quad (z, \theta_1 z), \quad (z, \theta_2 z), \ldots, \quad (z, \theta_{r-1} z)$$

les substitutions qui ne contiennent pas $x_0$; désignons par $\theta'_s z$ la fonction inverse de $\theta_s z$, la substitution $(z, \theta_s a^{u}\theta'_s z)$ est semblable à $(z, a^{u}z)$ et laisse la fonction invariable; ce sera une substitution différente de $(z, a^{u}z)$, à moins que l'on n'ait

$$\theta_s a^{u}\theta'_s z = \alpha^{u}z, \quad \text{d'où} \quad \theta_s(a^{u}z) = \alpha^{u}\theta_s z,$$

et alors $(z, \theta_s z)$ est de la forme (1).

Parmi les substitutions (2), il y en a qui s'effectuent sur moins de $p-1$ variables; soit $(z, \theta_\nu z)$ une telle substitution, et supposons qu'elle ne permute pas $x_\alpha$; si la substitution $(z, \theta_\nu z)$ est de la forme (1), la substitution $[z, \theta_\nu(z+\alpha)-\alpha]$ ne contient pas $x_0$ et n'est pas de la forme (1). Donc il existe au moins une substitution $(z, \theta_s a^{u}\theta'_s z)$ semblable à $(z, a^{u}z)$, et qui ne lui est pas identique.

Occupons-nous maintenant du cas particulier où la fonction transitive de $p$ quantités est invariable par toutes les substitutions $(z, a^2 z)$, ce qui arrive toutes les fois que $\frac{p-1}{2}$ est un nombre premier.

Soient

$$(z, z), \quad (z, \theta_1 z), \quad (z, \theta_2 z), \ldots \quad (z, \theta_{\varepsilon-1} z)$$

les substitutions qui ne permutent que $x_2, x_3, \ldots, x_{p-1}$. Les substitutions $(z, \theta_s a^2 \theta'_s z)$ sont des substitutions semblables à $(z, a^2 z)$.

Supposons d'abord que le nombre des substitutions qui ne contiennent pas $x_0$ et qui laissent la fonction invariable, soit $\frac{\varepsilon(p-1)}{2}$. Faisons dans l'expression $(z, \theta_s a^2 \theta'_s z)$ $a = 2, 3, \ldots, \frac{p-1}{2}$, et $s = 0, 1, 2, \ldots, \varepsilon - 1$, nous aurons $\frac{\varepsilon(p-3)}{2}$ substitutions de $p-1$ quantités semblables à $(z, a^2 z)$. Donc, comme le nombre total des substitutions faites sur $x_1, x_2, \ldots, x_{p-1}$ est $\frac{\varepsilon(p-1)}{2}$, et que le nombre de ces substitutions qui ont moins de $p-1$ variables est $> \varepsilon$, toutes les substitutions $(z, \theta_s a^2 \theta'_s z)$ ne sont pas distinctes, et on a

$$\theta_s a^2 \theta'_s z \equiv \theta_t b^2 \theta'_t z,$$

ou

$$\theta'_t \theta_s (a^2 z) \equiv b^2 \theta'_t \theta_s z;$$

d'où

$$\theta'_t \theta_s z \equiv A z^{\frac{p-1}{2}+\lambda} + B z^\lambda;$$

ainsi la fonction est invariable par au moins une substitution de la forme

$$\left(z, A z^{\frac{p-1}{2}+\lambda} + B z^\lambda\right).$$

En second lieu, supposons que le nombre des substitutions qui ne contiennent pas $x_0$ et qui laissent la fonction invariable soit $\varepsilon(p-1)$, auquel cas la fonction est deux fois transitive.

Soit $(z, \tau z)$ une substitution du second ordre qui contient $x_1$, et qui ne contient pas $x_0$; $\tau z$ n'étant pas une des fonctions

$$a^2 z, \quad a^2 \theta_1 z, \quad a^2 \theta_2 z, \ldots, \quad a^2 \theta_{\varepsilon-1} z,$$

et supposons que toutes les substitutions du second ordre qui ne contiennent pas $x_0$, soient données par les fonctions

$$a^2 z, \quad a^2 \theta_1 z, \quad a^2 \theta_2 z, \ldots, \quad a^2 \theta_{\varepsilon-1} z,$$
$$a^2 z, \quad \tau a^2 \theta_1 z, \quad \tau a^2 \theta_2 z, \ldots, \quad \tau a^2 \theta_{\varepsilon-1} z.$$

Si toutes les substitutions $(z, \theta_s a^2 \theta'_s z)$ et $(z, \theta_s \tau a^2 \tau' \theta'_s z)$ étaient différentes entre elles, elles seraient en nombre égal à $\varepsilon(p-3)$, puisque $a$ est susceptible des valeurs $2, 3, \ldots, \frac{p-1}{2}$, et $s$ des valeurs $0, 1, 2, \ldots, \varepsilon - 1$, et par conséquent on n'aurait que $2\varepsilon$ substitutions de moins de $p-1$ lettres; ce qui est impossible, puisqu'il n'y a pas de substitutions de moins de $\frac{p+1}{2}$ variables.

1° Supposons que l'on ait $\theta_s a^2 \theta'_s z \equiv \theta_t b^2 \theta'_t z$, on aura

$$\theta'_t \theta_s (a^2 z) \equiv b^2 \theta'_t \theta_s z;$$

2° Soit $\theta_s \tau a^2 \tau' \theta'_s z \equiv \theta_v b^2 \theta'_v z$, on aura

$$\theta'_v \theta_s \tau a^2 \tau' z \equiv b^2 \theta'_v \theta_s z,$$

$$\theta'_v \theta_s \tau (a^2 z) \equiv b^2 \theta'_v \theta_s \tau z.$$

3° Soit $\theta_s \tau a^2 \tau' \theta'_s z \equiv \theta_v \tau \alpha^2 \tau' \theta'_v z$, on aura

$$\theta'_v \theta_s \tau a^2 \tau' z \equiv \tau \alpha^2 \tau' \theta'_v \theta_s z,$$

$$\tau' \theta'_v \theta_s \tau a^2 \tau' z \equiv \alpha^2 \tau' \theta'_v \theta_s z,$$

$$\tau' \theta'_v \theta_s \tau (a^2 z) \equiv \alpha^2 \tau' \theta'_v \theta_s \tau z.$$

Donc parmi les substitutions qui ne contiennent pas $x_0$, il y en a au moins une $(z, \mu z)$ pour laquelle on a

$$\mu (a^2 z) \equiv \alpha^2 \mu z \quad \text{ou} \quad \mu z \equiv \mathrm{A} z^{\frac{p-1}{2}+\lambda} + \mathrm{B} z^{\lambda}.$$

En terminant cette étude des fonctions d'un nombre premier de quantités, nous ferons remarquer que l'on ne doit pas croire à l'existence d'un très-grand nombre de théorèmes généraux relatifs à *toutes* ces fonctions; car il existe des fonctions transitives d'un nombre premier de variables, qui ne proviennent nullement de ce que le nombre de leurs variables est premier, et qui devraient satisfaire à ces théorèmes. Je citerai pour exemple la fonction trois fois transitive de 17 va-

riables qui a 1.2.3... 14 valeurs, et qui doit son existence non à ce que 17 est un nombre premier, mais à ce que 17 est une puissance de nombre premier, plus 1.

---

## CHAPITRE V.

### DES FONCTIONS TRANSITIVES DE $n$ QUANTITÉS, $n$ ÉTANT QUELCONQUE.

Nous allons donner dans ce chapitre plusieurs classes de fonctions transitives d'un nombre quelconque de quantités. Mais comme le sujet que nous allons traiter ici est bien loin d'avoir le même intérêt que celui qui a fait l'objet des chapitres précédents, nous n'y donnerons pas tout ce que nous avons pu trouver, et nous nous contenterons d'énoncer quelques propositions qui sont toutes très-faciles à démontrer.

Les classes de fonctions que nous allons donner, renferment presque toutes les fonctions une seule fois transitives qui ont moins de douze lettres.

*Des fonctions cycliques.*

On appelle fonction cyclique une fonction qui reste invariable par une certaine substitution circulaire contenant toutes ses variables.

Désignons par $x_0$, $x_1$, $x_2$,..., $x_{n-1}$ les $n$ variables de la fonction. Si cette fonction n'est invariable par aucune substitution circulaire de toutes ses variables qui ne soit puissance de $(x_z, x_{z+1})$, cette fonction n'est invariable que par des substitutions de la forme $(x_z, x_{az+b})$; mais la réciproque n'est pas vraie, une fonction invariable seulement par les substitutions $(x_z, x_{az+b})$, n'est pas nécessairement une seule fois cyclique.

Soient $a$, $b$,..., $c$, des nombres différents par rapport au module $n$ et premiers à $n$, il y a une fonction cyclique de $n$ quantités invariable par les substitutions comprises dans la formule

$$(z, a^\alpha b^\beta \ldots c^\gamma z + m);$$

en particulier, on a une fonction cyclique de $n$ quantités invariable

par toutes les substitutions

$$(z, az + b),$$

$a$ étant premier à $n$, et qui a $\frac{1.2\ldots(n-1)}{\varphi(n)}$ valeurs, $\varphi(n)$ désignant combien il y a de nombres inférieurs et premiers à $n$.

Si $n$ est un nombre pair, l'expression $[z, z + (-1)^z]$ est une substitution régulière de $n$ variables qui peut s'écrire

$$(x_0 x_1)(x_2 x_3)(x_4 x_5)\ldots(x_{n-2} x_{n-1});$$

mais si $n$ est impair, cette expression n'est plus une substitution, car elle changerait $x_1$ et $x_{n-1}$ en $x_0$.

On voit d'après cela que si $n$ est un nombre pair, il existe une fonction cyclique de $n$ quantités ayant $\frac{1.2\ldots(n-1)}{n}$ valeurs, et invariable par toutes les substitutions

$$[z, z + m + l(-1)^z],$$

et qu'il y a aussi une fonction cyclique de ces quantités invariable par les substitutions

$$\left[z, a^\alpha b^\beta \ldots c^\gamma z + m + l(-1)^z\right].$$

Si $n$ est pair, il n'y a pas de fonctions cycliques invariables seulement par des substitutions de $n$ et de $n-1$ quantités. Si $n$ est impair, il existe au moins une de ces fonctions, savoir la fonction invariable par les substitutions $(z, \pm z + b)$.

*Des fonctions invariables par les substitutions*

$$\left(x_{y,z,\ldots,u}\, x_{y+\alpha,\, z+\beta,\ldots,\, u+\gamma}\right).$$

Soit $n = pqr\ldots t$; considérons l'expression $x_{a,b,c,\ldots,e}$ et convenons que l'on aura

$$x_{a,b,c,\ldots,e} = x_{a',b',c',\ldots,e'},$$

si l'on a

$$a' \equiv a \pmod{p}, \qquad b' \equiv b \pmod{q}, \qquad ,\ldots, \qquad e' \equiv e \pmod{t}.$$

L'expression $x_{a,b,c,\ldots,e}$ pourra représenter les $n$ variables. Désignons par

$$(\alpha) \qquad (x_{y,z,\ldots,u}\; x_{y+\alpha,z+\beta,\ldots,u+\gamma})$$

une substitution qui augmente tous les premiers indices de $\alpha$, tous les seconds indices de $\beta$, etc. En donnant à $\alpha, \beta, \ldots, \gamma$ toutes les valeurs dont ils sont susceptibles, on obtient des substitutions conjuguées entre elles, et qui laissent invariable une fonction transitive F qui a $1.2.3\ldots(n-1)$ valeurs.

Si $p, q, r, \ldots, t$ sont des nombres qui sont tous premiers entre eux, les substitutions $(\alpha)$ sont toutes les puissances d'une même substitution circulaire, de sorte que les substitutions peuvent s'écrire sous cette forme beaucoup plus simple $(x_z\, x_{z+m})$, les indices étant pris par rapport au module $n$.

En général, si l'on veut avoir toutes les fonctions d'un nombre donné $n$ de variables, telles que F, et si l'on veut que le nombre des indices soit le plus petit possible, on adoptera la règle suivante : On cherchera de combien de manières le nombre $n$ peut être décomposé en facteurs $p, q, r, \ldots, t$ tels, que $q$ soit un diviseur de $p$, $r$ un diviseur de $q$, et ainsi de suite. Autant il y aura de manières de décomposer ainsi le nombre $n$, autant il y aura de fonctions transitives différentes telles que F. On prendra un nombre d'indices égal au nombre des facteurs $p, q, r, \ldots, t$ et l'on prendra ces indices respectivement suivant ces nombres considérés comme modules.

Soit $n = mp$; il y a une fonction transitive de $n$ quantités qui a $\frac{1.2.3\ldots(n-1)}{m^{p-2}}$ valeurs, et qui est invariable par les substitutions que l'on obtient en prenant le premier des cycles

$$(A) \quad \begin{cases} (x_0^0\, x_1^0\, x_2^0\, x_3^0 \ldots x_{m-1}^0),\ (x_0^1\, x_1^1\, x_2^1 \ldots x_{m-1}^1), \\ (x_0^2\, x_1^2 \ldots x_{m-1}^2), \ldots, (x_0^{p-1}\, x_1^{p-1} \ldots x_{m-1}^{p-1}), \end{cases}$$

avec l'inverse de l'un quelconque des suivants, ni par la substitution

$$(\mathrm{B})\qquad \begin{cases} (x_0^0\, x_0^1\, x_0^2 \ldots x_0^{p-1})\,(x_1^0\, x_1^1\, x_1^2 \ldots x_1^{p-1}) \\ (x_2^0\, x_2^1\, x_2^2 \ldots x_2^{p-1}) \ldots (x_{m-1}^0\, x_{m-1}^1 \ldots x_{m-1}^{p-1}). \end{cases}$$

Il y a une seconde fonction transitive de $n$ quantités qui a $\frac{1.2.3\ldots(n-1)}{m^{p-2}}$ valeurs et qui n'est changée ni par les substitutions que l'on obtient en prenant le premier des cycles (A) avec l'un quelconque des cycles (A) de rang pair ou avec l'inverse d'un quelconque des cycles (A) de rang impair, ni par la substitution (B).

Soit $n = mn_1$; s'il existe une fonction transitive de $m$ quantités ayant $p$ valeurs, il existe aussi une fonction transitive de $n$ quantités qui a $\frac{1.2\ldots(n-1)}{1.2\ldots(m-1)}\,p$ valeurs.

Considérons la fonction transitive de $m$ quantités qui a $p$ valeurs; désignons ses $m$ quantités par $x_0, x_1, x_2, \ldots, x_{m-1}$ et supposons que toutes les substitutions qui ne changent pas cette fonction soient

$$(x_z x_z),\ (x_z x_{\varphi_1 z}),\ (x_z x_{\varphi_2 z}), \ldots, (x_z x_{\varphi_{r-1} z}).$$

Désignons par

$$x_0^0, x_1^0, x_2^0, \ldots, x_{m-1}^0, x_0^1, x_1^1, x_2^1, \ldots, x_{m-1}^1, \ldots, x_0^{n_1-1}, x_1^{n_1-1}, \ldots, x_{m-1}^{n_1-1},$$

$n$ quantités, et imaginons une fonction de ces quantités invariable par la substitution

$$(x_z^y\, x_z^{y+1})$$

et par les substitutions

$$(x_z^y x_z^y),\ (x_z^y x_{\varphi_1 z}^y),\ (x_z^y x_{\varphi_2 z}^y), \ldots, (x_z^y x_{\varphi_{r-1} z}^y),$$

et nous aurons la fonction dont il s'agit.

## SUR LA FORME

## $X^2 + Y^2 + Z^2 + 8T^2$ ;

PAR M. J. LIOUVILLE.

**1.** On demande une expression simple du nombre N des représentations d'un entier donné $n$ par la forme

$$X^2 + Y^2 + Z^2 + 8T^2,$$

c'est-à-dire du nombre N des solutions de l'équation

$$n = X^2 + Y^2 + Z^2 + 8T^2,$$

où X, Y, Z, T sont des entiers à volonté positifs, nuls ou négatifs. Cette question se rattache évidemment à celle que nous avons traitée dans le cahier de juillet en considérant l'équation

$$n = x^2 + y^2 + z^2 + 2t^2.$$

Le nombre $A(n)$ des solutions de cette dernière équation se compose en effet de deux parties $A_1(n)$, $A_2(n)$, la première relative aux valeurs impaires de $t$, la seconde aux valeurs paires ; et il est clair que N n'est autre chose que $A_2(n)$.

Comme $n$ peut être indifféremment pair ou impair, je ferai

$$n = 2^\alpha m,$$

$m$ étant impair et l'exposant $\alpha$ pouvant se réduire à zéro ; puis désignant par $d$ un diviseur quelconque de $m$ et par $\delta$ le diviseur conjugué en sorte que $m = d\delta$, je poserai, comme dans le cahier de juillet et

en me servant d'une notation bien connue de Legendre et de Jacobi :

$$\sum \left(\frac{2}{\delta}\right) d = S.$$

Cette somme S joue un rôle important dans nos formules. On sait d'ailleurs que

$$\left(\frac{2}{\delta}\right) = (-1)^{\frac{\delta^2-1}{8}}.$$

**2.** Soit d'abord $n$ impair, $n = m$. On aura

$$N = 6S,$$

si $n$ est de la forme $8k+1$ ou de la forme $8k-3$; mais

$$N = 4S,$$

si $n$ est de la forme $8k+3$; enfin

$$N = 0,$$

si $n$ est de la forme $8k-1$.

Soit, en second lieu, $n$ impairement pair, $n = 2m$. On aura dans ce cas

$$N = 12S,$$

quelle que soit la forme linéaire de $m$.

Soit, en dernier lieu, $n$ pairement pair, $n = 2^\alpha m$, $\alpha > 1$. On aura

$$N = 2(2^\alpha - 1)S,$$

si $m = 8k \pm 1$; mais

$$N = 2(2^\alpha + 1)S,$$

si $m = 8k \pm 3$.

**3.** La somme S s'exprime aussi par un produit au moyen des facteurs premiers dont $m$ se compose Soit $p$ un de ces facteurs et $\mu$ son exposant dans $m$, de façon qu'on puisse écrire

$$m = \prod (p^\mu).$$

On aura

$$S = \prod \left[p^\mu + \left(\frac{2}{p}\right) p^{\mu-1} + p^{\mu-2} + \left(\frac{2}{p}\right) p^{\mu-3} + \ldots\right],$$

les exposants de $p$ allant en décroissant jusqu'à zéro, et les coefficients étant alternativement 1 et $\left(\frac{2}{p}\right)$. Cette nouvelle manière d'exprimer S a ses avantages.

4. Nous venons de déterminer pour tout entier $n$ le nombre total N des solutions tant propres qu'impropres de l'équation

$$n = X^2 + Y^2 + Z^2 + 8T^2.$$

On pourrait aussi demander le nombre M des solutions *propres*, pour lesquelles l'unité seule divise à la fois les entiers X, Y, Z, T. Il faut alors substituer à la fonction S une autre fonction R que je définirai en écrivant

$$R = \prod \left[p^\mu + \left(\frac{2}{p}\right) p^{\mu-1}\right].$$

Cela posé, si $n$ est impair, $n = m$, on a

$$M = 6R,$$

quand $n$ est de l'une des deux formes $8k + 1$, $8k - 3$; mais

$$M = 4R,$$

quand $n$ est de la forme $8k + 3$; enfin

$$M = 0,$$

quand $n$ est de la forme $8k - 1$.

Pour $n$ impairement pair, $n = 2m$, on a

$$M = 12R,$$

quelle que soit la forme linéaire de $m$.

Le cas de $n$ pairement pair se décompose en trois autres suivant que l'on a $n = 4m$, ou $n = 8m$, ou enfin $n = 2^\alpha m$, $\alpha > 3$.

Pour $n = 4m$, je trouve

$$M = 6R,$$

quand $m$ est de l'une des deux formes $8k - 1$, $8k + 3$; mais

$$M = 4R,$$

quand $m$ est de la forme $8k - 3$; enfin

$$M = 0,$$

quand $m$ est de la forme $8k + 1$.

Pour $n = 8m$, il vient

$$M = 2R,$$

si $m = 8k \pm 1$; mais

$$M = 6R,$$

si $m = 8k \pm 3$.

Pour $n = 2^\alpha m$, $\alpha > 3$, on n'a qu'une seule formule :

$$M = 2^{\alpha - 1}.3R.$$

5. Ajoutons deux exemples. Soit d'abord

$$n = 125 = 5^3,$$

en sorte qu'il s'agisse d'un nombre impair de la forme $8k - 3$. Il viendra

$$S = 5^3 - 5^2 + 5 - 1 = 104$$

et

$$R = 5^3 - 5^2 = 100;$$

par suite

$$N = 6.104 = 624$$

et

$$M = 6.100 = 600.$$

Soit, en second lieu,

$$n = 252 = 2^2.3^2.7,$$

ce qui suppose

$$\alpha = 2, \quad m = 3^2.7,$$

partant

$$S = (3^2 - 3 + 1)(7 + 1) = 56$$

et

$$R = (3^2 - 3)(7 + 1) = 48.$$

On aura, $m$ étant de la forme $8k - 1$,

$$N = 2(2^2 - 1).56 = 336$$

et

$$M = 6.48 = 288.$$

SUR

# LES FONCTIONS ELLIPTIQUES;

PAR M. MATHET.

## I.

Parmi les propriétés des fonctions circulaires et exponentielles, il en est qui appartiennent aussi aux fonctions doublement périodiques dont les premières ne sont que des cas particuliers. C'est ainsi que l'équation

$$(1)\qquad \frac{\mathfrak{F}(x+y)}{\mathfrak{F}(x-y)}=\frac{F(x)f(y)+F(y)f(x)}{F(x)f(y)-F(y)f(x)},$$

dans laquelle $x$ et $y$ représentent deux variables indépendantes, est vérifiée quand $\frac{F(x)}{f(x)}=\operatorname{tang} x$, et l'est encore si $\frac{F(x)}{f(x)}$ est une fonction elliptique. De même l'équation

$$(2)\qquad \mathfrak{F}(x+y)=\frac{F'(x)f(y)+F(x)f'(y)}{1-K^2F(x)^2f(y)^2},$$

dans laquelle K représente une constante quelconque, est vérifiée si $F(x)=\operatorname{tang} x$ et $f(y)=\frac{1}{K}\cot y$, et l'est encore si $F(x)$ et $f(y)$ sont des fonctions elliptiques convenablement déterminées. Soit enfin l'équation

$$(3)\qquad \mathfrak{F}(x+y)=\frac{F(x)f(y)-F(y)f(x)}{F_1(x)f_1(y)-F_1(y)f_1(x)}.$$

Il est facile de montrer que si

$$\frac{F(x)}{f(x)}=\sin(x+p)\quad \text{et}\quad \frac{F_1(x)}{f_1(x)}=\sin(x+q),$$

$p$ et $q$ étant des constantes quelconques, on peut toujours déterminer $f(x)$ et $f_1(x)$ de telle sorte que cette équation soit vérifiée; on verra plus loin qu'il en est de même si $\frac{F(x)}{f(x)}$ et $\frac{F_1(y)}{f_1(y)}$ sont des fonctions elliptiques aux mêmes périodes.

On est alors conduit à se demander si ces fonctions doublement périodiques sont les solutions les plus générales des équations posées ci-dessus, ou si elles-mêmes ne sont que des cas particuliers de ces solutions. Telle est la question que je me propose d'examiner. Je déterminerai d'abord les fonctions qui peuvent vérifier l'équation

$$\mathcal{F}(x+y) = \frac{F_1(x)f_2(y) + F_2(x)f_1(y)}{F_3(x)f_4(y) + F_4(x)f_3(y)},$$

dont les équations (2) et (3) ne sont que des cas particuliers, et je résoudrai ensuite la même question pour l'équation

$$\frac{\mathcal{F}(x+y)}{\mathcal{F}_1(x-y)} = \frac{F(x)f_1(y) + f(x)F_1(y)}{F(x)f_1(y) - f(x)F_1(y)},$$

qui renferme également l'équation (1).

## II.

Soit l'équation

$$(1) \qquad \mathcal{F}(x+y) = \frac{F_1(x)f_2(y) + F_2(x)f_1(y)}{F_3(x)f_4(y) + F_4(x)f_3(y)}.$$

Si l'on pose

$$\frac{F_1(x)}{F_2(x)} = \varphi(x), \quad \frac{f_1(y)}{f_2(y)} = \psi(y), \quad \frac{F_3(x)}{F_4(x)} = \varphi_1(x),$$

$$\frac{f_3(y)}{f_4(y)} = \psi_1(y), \quad \frac{F_2(x)}{F_4(x)} = \mathcal{F}_1(x), \quad \frac{f_2(y)}{f_4(y)} = \mathcal{F}_2(y),$$

l'équation (1) devient

$$(2) \qquad \mathcal{F}(x+y) = \frac{\varphi(x) + \psi(y)}{\varphi_1(x) + \psi_1(y)} \mathcal{F}_1(x)\mathcal{F}_2(y).$$

Prenons les logarithmes des deux membres, différentions par rapport à $x$, et ensuite par rapport à $y$, et posons

$$F(x+y) = \frac{d^2 L \mathcal{F}(x+y)}{dx\,dy};$$

il vient

$$(3)\qquad \frac{\varphi'_1(x)\psi'_1(y)}{[\varphi_1(x)+\psi_1(y)]^2} - \frac{\varphi'(x)\psi'(y)}{[\varphi(x)+\psi(y)]^2} = F(x+y).$$

Soit $u = \frac{\varphi'\psi'}{(\varphi+\psi)^2}$: on trouve en différentiant

$$\frac{du}{dx} = \frac{\psi'}{\varphi+\psi}\left(\frac{\varphi''}{\varphi+\psi} - 2\frac{\varphi'^2}{(\varphi+\psi)^2}\right),$$

$$\frac{du}{dy} = \frac{\varphi'}{\varphi+\psi}\left(\frac{\psi''}{\varphi+\psi} - 2\frac{\psi'^2}{(\varphi+\psi)^2}\right),$$

$$\frac{d^2u}{dx\,dy} = \left[\frac{\varphi''}{\varphi+\psi} - 2\frac{\varphi'^2}{(\varphi+\psi)^2}\right]\left[\frac{\psi''}{\varphi+\psi} - 2\frac{\psi'^2}{(\varphi+\psi)^2}\right] + 2\frac{\varphi'^2\psi'^2}{(\varphi+\psi)^4};$$

d'où

$$(4)\qquad u\frac{d^2u}{dx\,dy} = \frac{du}{dx}\frac{du}{dy} + 2u^3.$$

L'équation (4) est évidemment vérifiée par la fonction

$$u_1 = \frac{\varphi'_1\psi'_1}{(\varphi_1+\psi_1)^2};$$

mais, en vertu de l'équation (3),

$$u_1 = F + u;$$

on peut donc remplacer, dans l'équation (4), $u$ par $F+u$. Si l'on élimine ensuite, par des différentiations, la fonction F et ses dérivées, il restera une équation aux différences partielles de $u$, qui déterminera cette fonction. Les calculs qui vont suivre auront pour objet de former, non pas précisément cette équation, mais un système d'équations équivalent, dont la discussion nous fournira la solution de la question.

Posons

$$\frac{du}{dx} - \frac{du}{dy} = f.$$

Si l'on différentie l'équation (4) par rapport à $x$ et par rapport à $y$, et si l'on retranche l'un de l'autre les deux résultats, on a

$$(5) \qquad u\frac{d^2 f}{dx\,dy} + f\frac{d^2 u}{dx\,dy} = \frac{du}{dx}\frac{df}{dy} + \frac{du}{dy}\frac{df}{dx} + 6u^2 f.$$

Posons encore

$$\frac{df}{dx} + \frac{df}{dy} = v.$$

Si l'on différentie l'équation (5) par rapport à $x$ et par rapport à $y$, et si l'on ajoute les deux résultats, on a

$$u\frac{d^2 v}{dx\,dy} + \left(\frac{du}{dx} + \frac{du}{dy}\right)\frac{d^2 f}{dx\,dy} + v\frac{d^2 u}{dx\,dy} + f\left(\frac{d^3 u}{dx^2\,dy} + \frac{d^3 u}{dx\,dy^2}\right)$$

$$= \left(\frac{d^2 u}{dx^2} + \frac{d^2 u}{dx\,dy}\right)\frac{df}{dy} + \left(\frac{d^2 u}{dx\,dy} + \frac{d^2 u}{dy^2}\right)\frac{df}{dx} + \frac{du}{dx}\frac{dv}{dy} + \frac{du}{dy}\frac{dv}{dx} + 6u^2 v$$

$$+ 12uf\left(\frac{du}{dx} + \frac{du}{dy}\right).$$

Mais

$$\left(\frac{d^2 u}{dx^2} + \frac{d^2 u}{dx\,dy}\right)\frac{df}{dy} + \left(\frac{d^2 u}{dx\,dy} + \frac{d^2 u}{dy^2}\right)\frac{df}{dx}$$

$$= \left(\frac{d^2 u}{dx^2} - \frac{d^2 u}{dx\,dy}\right)\frac{df}{dy} - \left(\frac{d^2 u}{dx\,dy} - \frac{d^2 u}{dy^2}\right)\frac{df}{dx} + 2\left(\frac{df}{dx} + \frac{df}{dy}\right)\frac{d^2 u}{dx\,dy}$$

$$= \frac{df}{dx}\frac{df}{dy} - \frac{df}{dy}\frac{df}{dx} + 2v\frac{d^2 u}{dx\,dy} = 2v\frac{d^2 u}{dx\,dy}.$$

Donc

$$(a) \quad \left\{\begin{aligned} &u\frac{d^2 v}{dx\,dy} - v\frac{d^2 u}{dx\,dy} + \left(\frac{du}{dx} + \frac{du}{dy}\right)\frac{d^2 f}{dx\,dy} + f\left(\frac{d^3 u}{dx^2\,dy} + \frac{d^3 u}{dx\,dy^2}\right) \\ &\qquad = \frac{du}{dx}\frac{dv}{dy} + \frac{du}{dy}\frac{dv}{dx} + 6u^2 v + 12uf\left(\frac{du}{dx} + \frac{du}{dy}\right).\end{aligned}\right.$$

Mais si l'on différentie l'équation (4) par rapport à $x$ et par rapport à $y$, et si l'on ajoute les deux résultats, on a

$$u\left(\frac{d^3 u}{dx^2 dy}+\frac{d^3 u}{dx\,dy^2}\right)+\left(\frac{du}{dx}+\frac{du}{dy}\right)\frac{d^2 u}{dx\,dy}$$
$$=\frac{du}{dx}\left(\frac{d^2 u}{dx\,dy}+\frac{d^2 u}{d^2 y}\right)+\frac{du}{dy}\left(\frac{d^2 u}{dx^2}+\frac{d^2 u}{dx\,dy}\right)+6u^2\left(\frac{du}{dx}+\frac{du}{dy}\right),$$

d'où

$$u\left(\frac{d^3 u}{dx^2 dy}+\frac{d^3 u}{dx\,dy^2}\right)=\frac{du}{dy}\frac{df}{dx}-\frac{du}{dx}\frac{df}{dy}+\left(\frac{du}{dx}+\frac{du}{dy}\right)\frac{d^2 u}{dx\,dy}+6u^2\left(\frac{du}{dx}+\frac{du}{dy}\right),$$

et, par conséquent, en multipliant l'équation ($a$) par $u$, et y substituant à la place de $u\left(\frac{d^3 u}{dx^2 dy}+\frac{d^3 u}{dx\,dy^2}\right)$ l'expression que l'on vient de trouver, et à la place de $u\frac{d^2 f}{dx\,dy}$ la valeur fournie par l'équation (5), on a

$$(b)\begin{cases} u^2\frac{d^2 v}{dx\,dy}-uv\frac{d^2 u}{dx\,dy}+\left(\frac{du}{dx}+\frac{du}{dy}\right)\left[\frac{du}{dx}\frac{df}{dy}+\frac{du}{dy}\frac{df}{dx}-f\frac{d^2 u}{dx\,dy}+6u^2 f\right] \\ \qquad +f\left[\frac{du}{dy}\frac{df}{dx}-\frac{du}{dx}\frac{df}{dy}+\left(\frac{du}{dx}+\frac{du}{dy}\right)\frac{d^2 u}{dx\,dy}+6u^2\left(\frac{du}{dx}+\frac{du}{dy}\right)\right] \\ \qquad =u\left(\frac{du}{dx}\frac{dv}{dy}+\frac{du}{dy}\frac{dv}{dx}\right)+6u^3 v+12u^2 f\left(\frac{du}{dx}+\frac{du}{dy}\right). \end{cases}$$

Mais on a, en se rappelant que $f=\frac{du}{dx}-\frac{du}{dy}$,

$$\left(\frac{du}{dx}+\frac{du}{dy}\right)\left(\frac{du}{dx}\frac{df}{dy}+\frac{du}{dy}\frac{df}{dx}\right)+f\left(\frac{du}{dy}\frac{df}{dx}-\frac{du}{dx}\frac{df}{dy}\right)$$
$$=\frac{df}{dy}\left[\left(\frac{du}{dx}\right)^2+\frac{du}{dx}\frac{du}{dy}-\left(\frac{du}{dx}\right)^2+\frac{du}{dx}\frac{du}{dy}\right]$$
$$+\frac{df}{dx}\left[\frac{du}{dx}\frac{du}{dy}+\left(\frac{du}{dy}\right)^2+\frac{du}{dx}\frac{du}{dy}-\left(\frac{du}{dy}\right)^2\right].$$

L'équation ($b$) devient donc

$$u^2\frac{d^2 v}{dx\,dy}-uv\frac{d^2 u}{dx\,dy}+2v\frac{du}{dx}\frac{du}{dy}=u\left(\frac{du}{dx}\frac{dv}{dy}+\frac{du}{dy}\frac{dv}{dx}\right)+6u^3 v.$$

Or l'équation (4) nous donne

$$\frac{du}{dx}\frac{du}{dy} = u\frac{d^2 u}{dx\,dy} - 2u^3;$$

si l'on fait cette substitution dans l'équation précédente et si l'on divise tous les termes par $u$, il vient

$$(6)\qquad u\frac{d^2 v}{dx\,dy} + v\frac{d^2 u}{dx\,dy} = \frac{du}{dx}\frac{dv}{dy} + \frac{du}{dy}\frac{dv}{dx} + 10u^2 v,$$

équation de même forme que l'équation (5).

Chacune des équations (5) et (6) va maintenant nous fournir une relation entre F, F' et la fonction $u$ et ses dérivées. Considérons d'abord l'équation (5). Si on la différentie par rapport à $x$ et par rapport à $y$, et si l'on retranche l'un de l'autre les deux résultats, on a

$$u\left(\frac{d^3 f}{dx^2\,dy} - \frac{d^3 f}{dx\,dy^2}\right) + 2f\frac{d^2 f}{dx\,dy} + \left(\frac{df}{dx} - \frac{df}{dy}\right)\frac{d^2 u}{dx\,dy}$$
$$= \frac{du}{dx}\left(\frac{d^2 f}{dx\,dy} - \frac{d^2 f}{dy^2}\right) + \frac{du}{dy}\left(\frac{d^2 f}{dx^2} - \frac{d^2 f}{dx\,dy}\right) + 2\frac{df}{dx}\frac{df}{dy} + 6u^2\left(\frac{df}{dx} - \frac{df}{dy}\right)$$
$$+ 12uf^2.$$

Multiplions tous les termes de cette équation par $f$, et, dans le premier membre, mettons à la place de $f\dfrac{d^2 u}{dx\,dy}$ sa valeur prise dans l'équation (5); il vient

$$uf\left(\frac{d^3 f}{dx^2\,dy} - \frac{d^3 f}{dx\,dy^2}\right)$$
$$+ 2f^2\frac{d^2 f}{dx\,dy} + \left(\frac{df}{dx} - \frac{df}{dy}\right)\left(\frac{du}{dx}\frac{df}{dy} + \frac{du}{dy}\frac{df}{dx} + 6u^2 f - u\frac{d^2 f}{dx\,dy}\right)$$
$$= f\frac{du}{dx}\left(\frac{d^2 f}{dx\,dy} - \frac{d^2 f}{dy^2}\right) + f\frac{du}{dy}\left(\frac{d^2 f}{dx^2} - \frac{d^2 f}{dx\,dy}\right) + 2f\frac{df}{dx}\frac{df}{dy}$$
$$+ 6u^2 f\left(\frac{df}{dx} - \frac{df}{dy}\right) + 12uf^3.$$

On peut simplifier cette équation en se rappelant que $f = \dfrac{du}{dx} - \dfrac{du}{dy}$;

elle devient alors

$$uf\left(\frac{d^3f}{dx^2dy}-\frac{d^3f}{dx\,dy^2}\right)-u\left(\frac{df}{dx}-\frac{df}{dy}\right)\frac{d^2f}{dx\,dy}$$
$$=f\frac{du}{dy}\frac{d^2f}{dx^2}-f\frac{du}{dx}\frac{d^2f}{dy^2}-f\left(\frac{du}{dx}-\frac{du}{dy}\right)\frac{d^2f}{dx\,dy}+\left(\frac{du}{dx}-\frac{du}{dy}\right)\frac{df}{dx}\frac{df}{dy}$$
$$-\frac{du}{dy}\left(\frac{df}{dx}\right)^2+\frac{du}{dx}\left(\frac{df}{dy}\right)^2+12uf^3,$$

ou bien

$$(7)\quad\left\{\begin{aligned}&u\left[f\left(\frac{d^3f}{dx^2dy}-\frac{d^3f}{dx\,dy^2}\right)-\left(\frac{df}{dx}-\frac{df}{dy}\right)\frac{d^2f}{dx\,dy}-12f^3\right]\\&\quad=\frac{du}{dy}\left[f\left(\frac{d^2f}{dx^2}+\frac{d^2f}{dx\,dy}\right)-\frac{df}{dx}\left(\frac{df}{dx}+\frac{df}{dy}\right)\right]\\&\quad-\frac{du}{dx}\left[f\left(\frac{d^2f}{dx\,dy}+\frac{d^2f}{dy^2}\right)-\frac{df}{dy}\left(\frac{df}{dy}+\frac{df}{dx}\right)\right].\end{aligned}\right.$$

L'équation (7), déduite de l'équation (4), est évidemment vérifiée si, à la place de $u$, on met $u_1$ ou $F+u$ qui lui est égale en vertu de l'équation (3). Or $f_1$ ou $\frac{du_1}{dx}-\frac{du_1}{dy}$ est égale à $f$ ou $\frac{du}{dx}-\frac{du}{dy}$, en vertu de cette même équation (3); donc si l'on fait cette substitution, il vient, en tenant compte de l'équation (7),

$$(8)\quad\left\{\begin{aligned}&F\left[f\left(\frac{d^3f}{dx^2dy}-\frac{d^3f}{dx\,dy^2}\right)-\left(\frac{df}{dx}-\frac{df}{dy}\right)\frac{d^2f}{dx\,dy}-12f^3\right]\\&=F'\left[f\left(\frac{d^2f}{dx^2}-\frac{d^2f}{dy^2}\right)-\left(\frac{df}{dx}-\frac{df}{dy}\right)\left(\frac{df}{dx}+\frac{df}{dy}\right)\right].\end{aligned}\right.$$

De l'équation (6) nous pouvons, par un calcul analogue, tirer une équation de même forme. Différentions l'équation (6) par rapport à $x$ et par rapport à $y$, et retranchons l'un de l'autre les deux résultats: il vient

$$u\left(\frac{d^3v}{dx^2dy}-\frac{d^3v}{dx\,dy^2}\right)+f\frac{d^2v}{dx\,dy}+\left(\frac{dv}{dx}-\frac{dv}{dy}\right)\frac{d^2u}{dx\,dy}+v\frac{d^2f}{dx\,dy}$$
$$=\frac{df}{dx}\frac{dv}{dy}+\frac{df}{dy}\frac{dv}{dx}+\frac{du}{dx}\left(\frac{d^2v}{dx\,dy}-\frac{d^2v}{dy^2}\right)+\frac{du}{dy}\left(\frac{d^2v}{dx^2}-\frac{d^2v}{dx\,dy}\right)+20uvf$$
$$+10u^2\left(\frac{dv}{dx}-\frac{dv}{dy}\right).$$

Je multiplie tous les termes par $v$, et je substitue à $10u^2v$ sa valeur prise dans l'équation (6); il vient

$$uv\left(\frac{d^3v}{dx^2dy}-\frac{d^3v}{dx\,dy^2}\right)+vf\frac{d^2v}{dx\,dy}+\left(\frac{dv}{dx}-\frac{dv}{dy}\right)v\frac{d^2u}{dx\,dy}+v^2\frac{d^2f}{dx\,dy}$$
$$=v\frac{df}{dx}\frac{dv}{dy}+v\frac{df}{dy}\frac{dv}{dx}+v\frac{du}{dy}\frac{d^2v}{dx^2}-v\frac{du}{dx}\frac{d^2v}{dy^2}+vf\frac{d^2v}{dx\,dy}+20uv^2f$$
$$+\left[u\frac{d^2v}{dx\,dy}+v\frac{d^2u}{dx\,dy}-\frac{du}{dx}\frac{dv}{dy}-\frac{du}{dy}\frac{dv}{dx}\right]\left(\frac{dv}{dx}-\frac{dv}{dy}\right).$$

Les termes $vf\frac{d^2v}{dx\,dy}$ et $v\left(\frac{dv}{dx}-\frac{dv}{dy}\right)\frac{d^2u}{dx\,dy}$, disparaissent dans les deux membres, et il reste

$$(9)\quad\left\{\begin{aligned}&u\left[v\left(\frac{d^3v}{dx^2dy}-\frac{d^3v}{dx\,dy^2}\right)-\left(\frac{dv}{dx}-\frac{dv}{dy}\right)\frac{d^2v}{dx\,dy}-20v^2f\right]\\&=\frac{du}{dy}\left[v\frac{d^2v}{dx^2}-\frac{dv}{dx}\left(\frac{dv}{dx}-\frac{dv}{dy}\right)\right]-\frac{du}{dx}\left[v\frac{d^2v}{dy^2}-\frac{dv}{dy}\left(\frac{dv}{dy}-\frac{dv}{dx}\right)\right]\\&-v^2\frac{d^2f}{dx\,dy}+v\left(\frac{df}{dx}\frac{dv}{dy}+\frac{df}{dy}\frac{dv}{dx}\right).\end{aligned}\right.$$

Cette équation est vérifiée quand on y remplace $u$ par $u_1$ ou par $F+u$ qui lui est égale en vertu de l'équation (3). D'ailleurs $f_1$ ou $\frac{du_1}{dx}-\frac{du_1}{dy}$ étant égale à $f$ ou $\frac{du}{dx}-\frac{du}{dy}$, il en résulte que $v_1$ ou $\frac{df_1}{dx}+\frac{df_1}{dy}$ est égale à $v$ ou $\frac{df}{dx}+\frac{df}{dy}$. On a donc, en faisant cette substitution, et tenant compte de l'équation (9),

$$(10)\quad\left\{\begin{aligned}&F\left[v\left(\frac{d^3v}{dx^2dy}-\frac{d^3v}{dx\,dy^2}\right)-\left(\frac{dv}{dx}-\frac{dv}{dy}\right)\frac{d^2v}{dx\,dy}-20v^2f\right]\\&=F'\left[v\left(\frac{d^2v}{dx^2}-\frac{d^2v}{dy^2}\right)-\left(\frac{dv}{dx}-\frac{dv}{dy}\right)\left(\frac{dv}{dx}+\frac{dv}{dy}\right)\right],\end{aligned}\right.$$

équation analogue à l'équation (8).

Les deux équations (8) et (10) que nous venons d'obtenir, si nous les divisons membre à membre, nous fournissent une équation aux différences partielles, qui détermine la fonction $u$. Mais cette équation est d'une forme trop compliquée pour que l'on puisse déterminer son

intégrale générale, nous la remplacerons donc par le système des équations (8) et (10) qui lui est équivalent, et nous discuterons ces deux équations après leur avoir donné une forme plus simple, au moyen des transformations qui vont suivre.

### III.

Si dans l'équation (8) on remplace le coefficient de F par sa valeur prise dans l'équation (7), il vient

$$F\left\{\begin{array}{l} \dfrac{du}{dy}\left[f\left(\dfrac{d^2f}{dx^2}+\dfrac{d^2f}{dx\,dy}\right)-\dfrac{df}{dx}\left(\dfrac{df}{dx}+\dfrac{df}{dy}\right)\right] \\ -\dfrac{du}{dx}\left[f\left(\dfrac{d^2f}{dx\,dy}+\dfrac{d^2f}{dy^2}\right)-\dfrac{df}{dy}\left(\dfrac{df}{dx}+\dfrac{df}{dy}\right)\right] \end{array}\right\}$$
$$= F'u\left[f\left(\frac{d^2f}{dx^2}-\frac{d^2f}{dy^2}\right)-\left(\frac{df}{dx}-\frac{df}{dy}\right)\left(\frac{df}{dx}+\frac{df}{dy}\right)\right].$$

Si l'on pose

$$\frac{1}{f}\left(\frac{df}{dx}+\frac{df}{dy}\right)=w,$$

cette équation se réduit à

$$(11)\qquad F\left(\frac{du}{dy}\frac{dw}{dx}-\frac{du}{dx}\frac{dw}{dy}\right)=F'u\left(\frac{dw}{dx}-\frac{dw}{dy}\right).$$

De même, si dans l'équation (10) on substitue au coefficient de F sa valeur prise dans l'équation (9), on a

$$F\left\{\begin{array}{l} \dfrac{du}{dy}\left[v\dfrac{d^2v}{dx^2}-\dfrac{dv}{dx}\left(\dfrac{dv}{dx}-\dfrac{dv}{dy}\right)\right]-\dfrac{du}{dx}\left[v\dfrac{d^2v}{dy^2}-\dfrac{dv}{dy}\left(\dfrac{dv}{dy}-\dfrac{dv}{dx}\right)\right] \\ \qquad\qquad -v^2\dfrac{d^2f}{dx\,dy}+v\left(\dfrac{df}{dx}\dfrac{dv}{dy}+\dfrac{df}{dy}\dfrac{dv}{dx}\right) \end{array}\right\}$$
$$= F'u\left[v\left(\frac{d^2v}{dx^2}-\frac{d^2v}{dy^2}\right)-\left(\frac{dv}{dx}-\frac{dv}{dy}\right)\left(\frac{dv}{dx}+\frac{dv}{dy}\right)\right].$$

Mais $v=wf$, d'où, en différentiant,

$$\frac{dv}{dx}=f\frac{dw}{dx}+w\frac{df}{dx},\quad \frac{d^2v}{dx^2}=f\frac{d^2w}{dx^2}+2\frac{dw}{dx}\frac{df}{dx}+w\frac{d^2f}{dx^2}.$$

Donc

$$v\frac{d^2v}{dx^2} - \left(\frac{dv}{dx}\right)^2 = f^2\left[w\frac{d^2w}{dx^2} - \left(\frac{dw}{dx}\right)^2\right] + w^2\left[f\frac{d^2f}{dx^2} - \left(\frac{df}{dx}\right)^2\right],$$

et de même

$$v\frac{d^2v}{dy^2} - \left(\frac{dv}{dy}\right)^2 = f^2\left[w\frac{d^2w}{dy^2} - \left(\frac{dw}{dy}\right)^2\right] + w^2\left[f\frac{d^2f}{dy^2} - \left(\frac{df}{dy}\right)^2\right].$$

On a aussi

$$\begin{aligned}
&\left(\frac{du}{dy} - \frac{du}{dx}\right)\frac{dv}{dx}\frac{dv}{dy} - v^2\frac{d^2f}{dx\,dy} + v\left(\frac{df}{dx}\frac{dv}{dy} + \frac{df}{dy}\frac{dv}{dx}\right)\\
&= -w^2 f\frac{df}{dx}\frac{df}{dy} - wf^2\frac{df}{dx}\frac{dw}{dy} - wf^2\frac{df}{dy}\frac{dw}{dx} - f^3\frac{dw}{dx}\frac{dw}{dy}\\
&\quad - w^2 f^2\frac{d^2f}{dx\,dy} + 2w^2 f\frac{df}{dx}\frac{df}{dy} + wf^2\frac{df}{dy}\frac{dw}{dx} + wf^2\frac{df}{dx}\frac{dw}{dy}\\
&= -w^2\left(\frac{du}{dx} - \frac{du}{dy}\right)\left(f\frac{d^2f}{dx\,dy} - \frac{df}{dx}\frac{df}{dy}\right) - f^2\left(\frac{du}{dx} - \frac{du}{dy}\right)\frac{dw}{dx}\frac{dw}{dy}.
\end{aligned}$$

L'équation trouvée ci-dessus devient donc

$$\begin{aligned}
&F\left\{\begin{aligned}
&\frac{du}{dy}\left\{\begin{aligned}
&f^2\left[w\frac{d^2w}{dx^2} - \left(\frac{dw}{dx}\right)^2 + \frac{dw}{dx}\frac{dw}{dy}\right]\\
&+ w^2\left[f\frac{d^2f}{dx^2} - \left(\frac{df}{dx}\right)^2 + f\frac{d^2f}{dx\,dy} - \frac{df}{dx}\frac{df}{dy}\right]
\end{aligned}\right\}\\
&-\frac{du}{dx}\left\{\begin{aligned}
&f^2\left[w\frac{d^2w}{dy^2} - \left(\frac{dw}{dy}\right)^2 + \frac{dw}{dx}\frac{dw}{dy}\right]\\
&+ w^2\left[f\frac{d^2f}{dy^2} - \left(\frac{df}{dy}\right)^2 + f\frac{d^2f}{dx\,dy} - \frac{df}{dx}\frac{df}{dy}\right]
\end{aligned}\right\}
\end{aligned}\right\}\\
&= F'u\left\{\begin{aligned}
&f^2\left[w\left(\frac{d^2w}{dx^2} - \frac{d^2w}{dy^2}\right) - \left(\frac{dw}{dx}\right)^2 + \left(\frac{dw}{dy}\right)^2\right]\\
&+ w^2\left[f\left(\frac{d^2f}{dx^2} - \frac{d^2f}{dy^2}\right) - \left(\frac{df}{dx}\right)^2 + \left(\frac{df}{dy}\right)^2\right]
\end{aligned}\right\},
\end{aligned}$$

équation qui, en vertu de l'équation (11), se réduit à

$$(12)\quad \begin{cases} F\left\{\frac{du}{dy}\left[w\frac{d^2w}{dx^2}-\left(\frac{dw}{dx}\right)^2+\frac{dw}{dx}\frac{dw}{dy}\right]-\frac{du}{dx}\left[w\frac{d^2w}{dy^2}-\left(\frac{dw}{dy}\right)^2+\frac{dw}{dx}\frac{dw}{dy}\right]\right\} \\ = F'u\left[w\left(\frac{d^2w}{dx^2}-\frac{d^2w}{dy^2}\right)-\left(\frac{dw}{dx}\right)^2+\left(\frac{dw}{dy}\right)^2\right]. \end{cases}$$

Soit maintenant

$$\frac{1}{w}=z,$$

l'équation (11) devient

$$(13)\qquad F\left(\frac{du}{dy}\frac{dz}{dx}-\frac{du}{dx}\frac{dz}{dy}\right)=F'u\left(\frac{dz}{dx}-\frac{dz}{dy}\right).$$

Mais de

$$\frac{1}{w}=z$$

on tire

$$-\frac{1}{w^2}\frac{dw}{dx}=\frac{dz}{dx}\quad \text{et}\quad -\frac{1}{w^2}\frac{d^2w}{dx^2}+\frac{2}{w^3}\left(\frac{dw}{dx}\right)^2=\frac{d^2z}{dx^2},$$

d'où

$$w\frac{d^2v}{dx^2}-\left(\frac{dw}{dx}\right)^2+\frac{dw}{dx}\frac{dw}{dy}=\frac{dw}{dx}\left(\frac{dw}{dx}+\frac{dw}{dy}\right)-w^3\frac{d^2z}{dx^2}.$$

L'équation (12) devient alors

$$F\left\{\left(\frac{du}{dy}\frac{dw}{dx}-\frac{du}{dx}\frac{dw}{dy}\right)\left(\frac{dw}{dx}+\frac{dw}{dy}\right)-w^3\left(\frac{du}{dy}\frac{d^2z}{dx^2}-\frac{du}{dx}\frac{d^2z}{dy^2}\right)\right\}$$
$$=F'u\left[\left(\frac{dw}{dx}+\frac{dw}{dy}\right)\left(\frac{dw}{dx}-\frac{dw}{dy}\right)-w^3\left(\frac{d^2z}{dx^2}-\frac{d^2z}{dy^2}\right)\right],$$

équation qui, en vertu de l'équation (11), se réduit à

$$(14)\qquad F\left(\frac{du}{dy}\frac{d^2z}{dx^2}-\frac{du}{dx}\frac{d^2z}{dy^2}\right)=F'u\left(\frac{d^2z}{dx^2}-\frac{d^2z}{dy^2}\right).$$

Enfin nous poserons $\frac{u}{F}=t$, et les équations (13) et (14) deviendront

alors

$$(15)\qquad \frac{dt}{dx}\frac{dz}{dy} - \frac{dt}{dy}\frac{dz}{dx} = 0,$$

$$(16)\qquad \frac{dt}{dx}\frac{d^2z}{dy^2} - \frac{dt}{dy}\frac{d^2z}{dx^2} = 0.$$

Nous allons maintenant discuter ces deux équations, et nous verrons que, parmi les diverses solutions qu'elles peuvent admettre, il n'en est que deux qui conviennent à la question, savoir : $t =$ constante ou $z =$ constante.

## IV.

Considérons d'abord l'équation (15)

$$\frac{dt}{dx}\frac{dz}{dy} - \frac{dt}{dy}\frac{dz}{dx} = 0.$$

$z$ peut être considérée comme une fonction de $t$ et de $x$ ; alors on doit avoir

$$\frac{dt}{dx}\frac{dz}{dt}\frac{dt}{dy} - \frac{dt}{dy}\left(\frac{dz}{dx} + \frac{dz}{dt}\frac{dt}{dx}\right) = 0, \quad \text{ou} \quad \frac{dt}{dy}\frac{dz}{dx} = 0.$$

Si $\frac{dt}{dy} = 0$, $t$ est indépendante de $y$ ; soit

$$t = \varphi(x), \quad \text{ou} \quad u = \varphi(x)\,F(x+y).$$

Il en résulte

$$\frac{du}{dx} = \varphi' F + \varphi F', \quad \frac{du}{dy} = \varphi F', \quad \frac{d^2u}{dx\,dy} = \varphi' F' + \varphi F'';$$

donc, en vertu de l'équation (4),

$$\varphi F(\varphi' F' + \varphi F'') = \varphi\varphi' F F' + \varphi^2 F'^2 + 2\varphi^3 F^3 \quad \text{ou} \quad \frac{FF'' - F'^2}{F^3} = 2\varphi.$$

Pour que $\varphi$, fonction de $x$, soit identique à une fonction de $x + y$, il faut qu'elle se réduise à une constante ; donc $t =$ constante.

Si $\frac{dt}{dy}$ n'est pas nulle, il faut que $\frac{dz}{dx}$ le soit, c'est-à-dire que $z$ soit une fonction de $t$, $z = \varpi(t)$. Cette fonction doit en outre satisfaire à l'équation (16). Or

$$\frac{dz}{dx} = \varpi' \frac{dt}{dx}, \quad \frac{d^2 z}{dx^2} = \varpi' \frac{d^2 t}{dx^2} + \varpi'' \left(\frac{dt}{dx}\right)^2, \quad \cdots$$

Donc on doit avoir

$$\frac{dt}{dy}\left[\varpi'' \left(\frac{dt}{dx}\right)^2 + \varpi' \frac{d^2 t}{dx^2}\right] - \frac{dt}{dx}\left[\varpi'' \left(\frac{dt}{dy}\right)^2 + \varpi' \frac{d^2 t}{dy^2}\right] = 0,$$

ou

$$(17) \qquad \varpi' \left(\frac{dt}{dy}\frac{d^2 t}{dx^2} - \frac{dt}{dx}\frac{d^2 t}{dy^2}\right) + \varpi'' \frac{dt}{dx}\frac{dt}{dy}\left(\frac{dt}{dx} - \frac{dt}{dy}\right) = 0.$$

$t$ étant égale à $\frac{u}{F}$, on a

$$\frac{dt}{dy} = \frac{1}{F^2}\left(F \frac{du}{dy} - F' u\right),$$

et

$$\frac{d^2 t}{dx^2} = \frac{1}{F^3}\left(F^2 \frac{d^2 u}{dx^2} - 2 F F' \frac{du}{dx} - F F'' u + 2 F'^2 u\right).$$

Donc

$$\frac{dt}{dy}\frac{d^2 t}{dx^2} = \frac{1}{F^5}\left[F^3 \frac{du}{dy}\frac{d^2 u}{dx^2} - 2 F^2 F' \frac{du}{dx}\frac{du}{dy} + (2 F'^2 - F F'') F u \frac{du}{dy} - F^2 F' u \frac{d^2 u}{dx^2}\right.$$
$$\left. + 2 F F'^2 u \frac{du}{dx} - (2 F'^2 - F F'') F' u^2\right];$$

et, de même,

$$\frac{dt}{dx}\frac{d^2 t}{dy^2} = \frac{1}{F^5}\left[F^3 \frac{du}{dx}\frac{d^2 u}{dy^2} - 2 F^2 F' \frac{du}{dy}\frac{du}{dx} + (2 F'^2 - F F'') F u \frac{du}{dx} - F^2 F' u \frac{d^2 u}{dy^2}\right.$$
$$\left. + 2 F F'^2 u \frac{du}{dy} - (2 F'^2 - F F'') F' u^2\right].$$

Donc, en retranchant,

$$(18)\quad \left\{\begin{aligned} \frac{dt}{dy}\frac{d^2t}{dx^2}-\frac{dt}{dx}\frac{d^2t}{dy^2}=\frac{1}{F^3}\Big[&F\left(\frac{du}{dy}\frac{d^2u}{dx^2}-\frac{du}{dx}\frac{d^2u}{dy^2}\right)+F''u\left(\frac{du}{dx}-\frac{du}{dy}\right)\\ &-F'u\left(\frac{d^2u}{dx^2}-\frac{d^2u}{dy^2}\right)\Big].\end{aligned}\right.$$

Reprenons l'équation (4)

$$u\frac{d^2u}{dx\,dy}=\frac{du}{dx}\frac{du}{dy}+2u^3.$$

Si on la différentie par rapport à $x$ et par rapport à $y$, et si l'on retranche l'un de l'autre les deux résultats, on a

$$(19)\qquad u\left(\frac{d^3u}{dx^2dy}-\frac{d^3u}{dx\,dy^2}\right)=\frac{du}{dy}\frac{d^2u}{dx^2}-\frac{du}{dx}\frac{d^2u}{dy^2}+6u^2\left(\frac{du}{dx}-\frac{du}{dy}\right).$$

Cette équation devant être vérifiée quand on y remplace $u$ par $u_1$ ou par $F+u$, on a

$$\begin{aligned}(F+u)\left(\frac{d^3u}{dx^2dy}-\frac{d^3u}{dx\,dy^2}\right)=\left(F'+\frac{du}{dy}\right)\left(F''+\frac{d^2u}{dx^2}\right)-\left(F'+\frac{du}{dx}\right)\left(F''+\frac{d^2u}{dy^2}\right)&\\ +6(F+u)^2\left(\frac{du}{dx}-\frac{du}{dy}\right)&,\end{aligned}$$

équation qui, en vertu de l'équation (19), se réduit à

$$\begin{aligned}F\left(\frac{d^3u}{dx^2dy}-\frac{d^3u}{dx\,dy^2}\right)=F'\left(\frac{d^2u}{dx^2}-\frac{d^2u}{dy^2}\right)-F''\left(\frac{du}{dx}-\frac{du}{dy}\right)&\\ +6F(F+2u)\left(\frac{du}{dx}-\frac{du}{dy}\right)&,\end{aligned}$$

d'où, en remplaçant le coefficient de F dans le premier membre par sa valeur prise dans l'équation (19),

$$\begin{aligned}F\left(\frac{du}{dy}\frac{d^2u}{dx^2}-\frac{du}{dx}\frac{d^2u}{dy^2}\right)+6u^2F\left(\frac{du}{dx}-\frac{du}{dy}\right)=F'u\left(\frac{d^2u}{dx^2}-\frac{d^2u}{dy^2}\right)-F''u\left(\frac{du}{dx}-\frac{du}{dy}\right)&\\ +6Fu(F+2u)\left(\frac{du}{dx}-\frac{du}{dy}\right)&.\end{aligned}$$

L'équation (18) se réduit donc à

$$\frac{dt}{dy}\frac{d^2t}{dx^2}-\frac{dt}{dx}\frac{d^2t}{dy^2}=\frac{6u(F+u)}{F^2}\left(\frac{du}{dx}-\frac{du}{dy}\right)=\frac{6u(F+u)}{F}\left(\frac{dt}{dx}-\frac{dt}{dy}\right),$$

et l'équation (17) devient

$$\left(\frac{dt}{dx}-\frac{dt}{dy}\right)\left[\frac{6\varpi' u(F+u)}{F}+\varpi''\frac{dt}{dx}\frac{dt}{dy}\right]=0.$$

Si $\frac{dt}{dx}-\frac{dt}{dy}=0$, $t$ est une fonction de $x+y$, et il en est de même de $u$, solution déjà mentionnée. Supposons donc qu'on ait

(20) $$\frac{6\varpi' u(F+u)}{F}+\varpi''\frac{dt}{dx}\frac{dt}{dy}=0.$$

Mais

$$\frac{dt}{dx}\frac{dt}{dy}=\frac{1}{F^4}\left[F^2\frac{du}{dx}\frac{du}{dy}-FF'u\left(\frac{du}{dx}+\frac{du}{dy}\right)+F'^2u^2\right].$$

De plus, l'équation

$$u\frac{d^2u}{dx\,dy}=\frac{du}{dx}\frac{du}{dy}+2u^3,$$

si l'on y remplace $u$ par $F+u$, nous donne

$$F''(F+u)+F\frac{d^2u}{dx\,dy}=F'^2+F'\left(\frac{du}{dx}+\frac{du}{dy}\right)+2F^3+6Fu(F+u),$$

ou, en multipliant tous les termes par $u$, et remplaçant $u\frac{d^2u}{dx\,dy}$ par $\frac{du}{dx}\frac{du}{dy}+2u^3$,

$$F\frac{du}{dx}\frac{du}{dy}-F'u\left(\frac{du}{dx}+\frac{du}{dy}\right)$$
$$=F'^2u-F''u(F+u)+2F^3u+6Fu^2(F+u)-2Fu^3;$$

donc

$$\frac{dt}{dx}\frac{dt}{dy}=\frac{1}{F^4}\left[FF'^2u-FF''u(F+u)+2F^4u+6F^2u^2(F+u)\right.$$
$$\left.-2F^2u^3+F'^2u^2\right].$$

ou

$$\frac{dt}{dx}\frac{dt}{dy} = \frac{1}{F^4} u(F+u)[F'^2 - FF'' + 2F^2(F-u) + 6F^2u]$$
$$= \frac{u(F+u)}{F^4}[F'^2 - FF'' + 2F^3 + 4F^2u].$$

Donc l'équation (20) devient

$$\frac{6\varpi' u(F+u)}{F} + \frac{\varpi'' u(F+u)}{F^4}[F'^2 - FF'' + 2F^3 + 4F^2u] = 0,$$

ou, en divisant par $\frac{u(F+u)}{F}$, et remarquant que $\frac{u}{F} = t$,

$$6\varpi' + \frac{\varpi''}{F^3}(F'^2 - FF'' + 2F^3 + 4F^3 t) = 0.$$

Or $\varpi'$ et $\varpi''$ sont des fonctions de $t$, donc il faut que $t$ soit une fonction de F et de ses dérivées, et par conséquent que $u$ soit une fonction de $x+y$, solution déjà obtenue; à moins que $\varpi'$ et $\varpi''$ ne soient identiquement nulles, auquel cas $\varpi$ est une constante.

Donc, pour que l'équation (3) soit vérifiée, c'est-à-dire pour que $u_1 - u = F(x+y)$, il faut, ou que $u$ et $u_1$ soient des fonctions de $x+y$, ou que $z = \frac{\frac{du}{dx} - \frac{du}{dy}}{\frac{d^2u}{dx^2} - \frac{d^2u}{dy^2}}$ soit égale à une constante, ainsi que la fonction analogue $z_1$.

Il nous reste à voir si ces conditions sont suffisantes, c'est-à-dire si les fonctions $\varphi$, $\psi$, $\varphi_1$ et $\psi_1$ qu'elles déterminent, satisfont toujours à l'équation (3); après quoi nous aurons encore à voir si elles satisfont à l'équation (2) et par conséquent à l'équation (1).

## V.

Si $u = \frac{\varphi'\psi'}{(\varphi+\psi)^2}$ est une fonction de $x+y$, on doit avoir

$$\frac{du}{dx} - \frac{du}{dy} = 0,$$

ou

$$\frac{\psi'}{\varphi+\psi}\left(\frac{\varphi''}{\varphi+\psi} - 2\frac{\varphi'^2}{(\varphi+\psi)^2}\right) - \frac{\varphi'}{\varphi+\psi}\left(\frac{\psi''}{\varphi+\psi} - 2\frac{\psi'^2}{(\varphi+\psi)^2}\right) = 0,$$

d'où

$$\frac{\varphi''}{\varphi'} - \frac{\psi''}{\psi'} - 2\,\frac{\varphi' - \psi'}{\varphi + \psi} = 0.$$

Posons

$$\frac{\varphi''}{\varphi'} = 2\varpi(x), \quad \frac{\psi''}{\psi'} = 2\theta(y);$$

on aura

$$\varphi' - \psi' = (\varpi - \theta)(\varphi + \psi).$$

D'où, en différentiant par rapport à $x$, puis par rapport à $y$,

$$\varphi'' = \varpi'(\varphi + \psi) + (\varpi - \theta)\varphi', \quad 0 = \varpi'\psi' - \theta'\varphi', \quad \frac{\varpi'}{\varphi'} = \frac{\theta'}{\psi'}.$$

Pour que ces deux fonctions, dont l'une ne dépend que de $x$ et l'autre ne dépend que de $y$, soient égales, il faut que chacune d'elles soit égale à une constante A. De $\frac{\varpi'}{\varphi'} = \mathrm{A}$ on tire $\varpi = \mathrm{A}\varphi + \mathrm{B}$, ou $\varphi'' = 2\mathrm{A}\varphi\varphi' + 2\mathrm{B}\varphi'$; d'où

$$\varphi' = \mathrm{A}\varphi^2 + 2\mathrm{B}\varphi + \mathrm{C};$$

on aura de même

$$\psi' = \mathrm{A}\psi^2 + 2\mathrm{B}_1\psi + \mathrm{C}_1.$$

Pour que ces valeurs vérifient l'équation

$$\frac{\varphi''}{\varphi'} - \frac{\psi''}{\psi'} - 2\,\frac{\varphi' - \psi'}{\varphi + \psi} = 0,$$

il faut que l'on ait identiquement

$$(2\mathrm{A}\varphi + 2\mathrm{B})(\varphi + \psi) - 2\mathrm{A}\varphi^2 - 4\mathrm{B}\varphi - 2\mathrm{C}$$
$$= (2\mathrm{A}\psi + 2\mathrm{B}_1)(\varphi + \psi) - 2\mathrm{A}\psi^2 - 4\mathrm{B}_1\psi - 2\mathrm{C}_1,$$

ou

$$2\mathrm{B}\psi - 2\mathrm{B}\varphi - 2\mathrm{C} = 2\mathrm{B}_1\varphi - 2\mathrm{B}_1\psi - 2\mathrm{C}_1.$$

ce qui exige que

$$\mathrm{B} + \mathrm{B}_1 = 0, \quad \text{et} \quad \mathrm{C} = \mathrm{C}_1.$$

Donc

$$\varphi' = A\varphi^2 + 2B\varphi + C, \quad \psi' = A\psi^2 - 2B\psi + C.$$

Désignons par $a_0$ et $a_1$ les deux racines de l'équation

$$A\varphi^2 + 2B\varphi + C = 0;$$

celles de l'équation

$$A\psi^2 - 2B\psi + C = 0$$

seront $-a_0$ et $-a_1$. On aura

$$\frac{\varphi'}{A(\varphi - a_0)(\varphi - a_1)} = 1, \quad \text{ou} \quad \frac{1}{A(a_0 - a_1)}\left[\frac{\varphi'}{\varphi - a_0} - \frac{\varphi'}{\varphi - a_1}\right] = 1,$$

d'où

$$\frac{1}{A(a_0 - a_1)} L\frac{\varphi - a_0}{\varphi - a_1} = x + p,$$

$p$ étant une constante arbitraire.

Soit $A(a_0 - a_1) = 2m$, il vient

$$\frac{\varphi - a_0}{\varphi - a_1} = e^{2m(x+p)}, \quad \varphi = \frac{a_1 e^{m(x+p)} - a_0 e^{-m(x+p)}}{e^{m(x+p)} - e^{-m(x+p)}}.$$

On aura de même

$$\psi = \frac{a_1 e^{-m(y+q)} - a_0 e^{m(y+q)}}{e^{m(y+q)} - e^{-m(y+q)}},$$

et, par conséquent,

$$\varphi + \psi = \frac{(a_1 - a_0)\left[e^{m(x+y+p+q)} - e^{-m(x+y+p+q)}\right]}{\left[e^{m(x+p)} - e^{-m(x+p)}\right]\left[e^{m(y+q)} - e^{-m(y+q)}\right]}.$$

On voit par là que si l'on prend pour $\varphi_1$ et pour $\psi_1$ des valeurs de même forme, déterminées par les équations

$$\varphi'_1 = a\varphi_1^2 + 2b\varphi_1 + c \quad \text{et} \quad \psi'_1 = a\psi_1^2 - 2b\psi_1 + c,$$

$a$, $b$ et $c$ étant des constantes quelconques, le rapport $\frac{\varphi + \psi}{\varphi_1 + \psi_1}$ sera égal

à une fonction de $x+y$, multipliée par le produit de deux fonctions, l'une dépendant de $x$ seulement, l'autre de $y$ seulement ; par conséquent l'équation (2) sera vérifiée.

## VI.

Soit maintenant

$$z = \frac{f}{\frac{df}{dx} + \frac{df}{dy}} = \frac{1}{2m},$$

d'où

$$\frac{1}{f}\frac{df}{dx} + \frac{1}{f}\frac{df}{dy} = 2m,$$

ou

$$\frac{d.[\mathrm{L}f - m(x+y)]}{dx} + \frac{d.[\mathrm{L}f - m(x+y)]}{dy} = 0.$$

Il en résulte

$$\mathrm{L}f - m(x+y) = \mathfrak{F}(x-y), \quad \text{ou} \quad f = e^{m(x+y)}\mathfrak{F}_1(x-y).$$

Mais

$$f = \frac{du}{dx} - \frac{du}{dy};$$

donc

$$\frac{d.\left[u - e^{m(x+y)}\mathfrak{F}_2(x-y)\right]}{dx} - \frac{d.\left[u - e^{m(x+y)}\mathfrak{F}_2(x-y)\right]}{dy} = 0,$$

$\mathfrak{F}_1(x-y)$ étant la dérivée de $2\mathfrak{F}_2(x-y)$. Donc, si $\varpi$ et $\theta$ représentent deux fonctions arbitraires, l'une de $x+y$, l'autre de $x-y$, on doit avoir

$$u = \varpi(x+y) - e^{m(x+y)}\theta(x-y).$$

Soient

$$x+y = \alpha, \qquad x-y = \beta;$$

l'équation

$$u\frac{d^2u}{dx\,dy} = \frac{du}{dx}\frac{du}{dy} + 2u^3$$

devient

$$u\left(\frac{d^2u}{d\alpha^2}-\frac{d^2u}{d\beta^2}\right)=\left(\frac{du}{d\alpha}\right)^2-\left(\frac{du}{d\beta}\right)^2+2u^3.$$

Mais

$$\frac{du}{d\alpha}=\varpi'-me^{m\alpha}\theta,\quad \frac{d^2u}{d\alpha^2}=\varpi''-m^2e^{m\alpha}\theta,$$

$$\frac{du}{d\beta}=-e^{m\alpha}\theta',\qquad \frac{d^2u}{d\beta^2}=-e^{m\alpha}\theta'';$$

donc

$$(21)\quad \left\{\begin{aligned}(\varpi-e^{m\alpha}\theta)(\varpi''-m^2e^{m\alpha}\theta+e^{m\alpha}\theta'')=\varpi'^2-2\varpi'me^{m\alpha}\theta\\ +m^2e^{2m\alpha}\theta^2-e^{2m\alpha}\theta'^2+2(\varpi-e^{m\alpha}\theta)^3.\end{aligned}\right.$$

Ordonnons par rapport à $e^{m\alpha}$:

$$\begin{aligned}(\varpi\varpi''-\varpi'^2-2\varpi^3)-e^{m\alpha}(\varpi''\theta+\varpi\theta m^2-2\varpi'\theta m-6\varpi^2\theta-\varpi\theta'')\\ +e^{2m\alpha}(\theta'^2-\theta\theta''-6\varpi\theta^2)+2\theta^3e^{3m\alpha}=0.\end{aligned}$$

Différentions par rapport à $\beta$, et divisons tous les termes par $e^{m\alpha}$ :

$$\begin{aligned}(2\varpi'm+6\varpi^2-\varpi''-m^2\varpi)\theta'+\varpi\theta'''\\ +e^{m\alpha}(\theta'\theta''-\theta\theta'''-12\varpi\theta\theta')+6\theta^2\theta'e^{2m\alpha}=0.\end{aligned}$$

Différentions de nouveau par rapport à $\beta$ :

$$\begin{aligned}(2\varpi'm+6\varpi^2-\varpi''-m^2\varpi)\theta''+\varpi\theta^{\text{iv}}\\ +e^{m\alpha}[\theta''^2-\theta\theta^{\text{iv}}-12\varpi(\theta'^2+\theta\theta'')]+6e^{2m\alpha}(\theta^2\theta''+2\theta\theta'^2)=0.\end{aligned}$$

Multiplions la dernière équation par $\theta'$, la précédente par $\theta''$, et retranchons l'un de l'autre les deux résultats ; il vient

$$-\varpi(\theta'\theta^{\text{iv}}-\theta''\theta''')+e^{m\alpha}[\theta(\theta'\theta^{\text{iv}}-\theta''\theta''')+12\varpi\theta'^3]-6e^{2m\alpha}.2\theta\theta'^3=0,$$

ou

$$(\varpi-\theta e^{m\alpha})(\theta'\theta^{\text{iv}}-\theta''\theta'''-12\theta'^3e^{m\alpha})=0.$$

Or $\varpi - e^{m\alpha}$, qui n'est autre chose que $u$, ne peut être nulle, donc le second facteur doit l'être. Mais $\theta$ et ses dérivées sont des fonctions de $\beta$ : donc pour que ce second facteur soit nul identiquement, il faut que la constante $m$ soit nulle, c'est-à-dire que

$$u = \varpi(x+y) - \theta(x-y).$$

Cette condition détermine les fonctions $\varpi$ et $\theta$, ainsi que les fonctions $\varphi$ et $\psi$. D'abord l'équation (21), si l'on fait $m = 0$, devient

$$(22) \qquad (\varpi - \theta)(\varpi'' + \theta'') = \varpi'^2 - \theta'^2 + 2(\varpi - \theta)^3.$$

De cette équation on tire

$$\varpi''' = \frac{(\varpi - \theta)[2\varpi'\varpi'' + 6\varpi'(\varpi-\theta)^2] - \varpi'[\varpi'^2 - \theta'^2 + 2(\varpi - \theta)^3]}{(\varpi - \theta)^2},$$

$$\frac{\varpi'''}{\varpi'} - 12\varpi = \frac{2(\varpi - \theta)\varpi'' - (\varpi'^2 - \theta'^2) + 4(\varpi - \theta)^3 - 12\varpi(\varpi - \theta)^2}{(\varpi - \theta)^2}.$$

L'équation (22) ne changeant pas quand on change $\varpi$ en $\theta$ et $\theta$ en $\varpi$, on aura de même

$$\frac{\theta'''}{\theta'} - 12\theta = \frac{-2(\varpi - \theta)\theta'' + \varpi'^2 - \theta'^2 - 4(\varpi - \theta)^3 - 12\theta(\varpi - \theta)^2}{(\varpi - \theta)^2};$$

et, par conséquent,

$$\frac{\varpi'''}{\varpi'} - 12\varpi - \left(\frac{\theta'''}{\theta'} - 12\theta\right) = \frac{2(\varpi - \theta)(\varpi'' + \theta'') - 2(\varpi'^2 - \theta'^2) - 4(\varpi - \theta)^3}{(\varpi - \theta)^2}.$$

Le second membre est nul, en vertu de l'équation (22); donc les fonctions $\frac{\varpi'''}{\varpi'} - 12\varpi$ et $\frac{\theta'''}{\theta'} - 12\theta$, qui ne dépendent, la première que de $\alpha$, la seconde que de $\beta$, doivent être égales à une constante A. Soit

$$\frac{\varpi'''}{\varpi'} - 12\varpi = A, \quad \varpi''' = 12\varpi\varpi' + A\varpi', \quad \varpi'' = 6\varpi^2 + A\varpi + \frac{B}{2};$$

multiplions par $2\varpi'$, et intégrons de nouveau :

$$\varpi'^2 = 4\varpi^3 + A\varpi^2 + B\varpi + C.$$

On aura de même

$$\theta'^2 = 4\theta^3 + A\theta^2 + B_1\theta + C_1.$$

Ces fonctions $\varpi$ et $\theta$ devant vérifier l'équation (22), on doit avoir

$$(\varpi - \theta)\left(6\varpi^2 + A\varpi + \frac{B}{2} + 6\theta^2 + A\theta + \frac{B_1}{2}\right)$$
$$= 4\varpi^3 + A\varpi^2 + B\varpi + C - 4\theta^3 - A\theta^2 - B_1\theta - C_1 + 2(\varpi - \theta)^3.$$

Si l'on développe cette équation, elle se réduit à

$$\frac{B - B_1}{2}(\varpi + \theta) + C - C_1 = 0,$$

ce qui exige que $B = B_1$ et $C = C_1$.

On doit donc avoir, en définitive,

$$\varpi'^2 = 4\varpi^3 + A\varpi^2 + B\varpi + C \quad \text{et} \quad \theta'^2 = 4\theta^3 + A\theta^2 + B\theta + C.$$

Donc $\theta(x)$ est égale, soit à $\varpi(x)$, soit à $\varpi(-x)$, et la fonction $\varpi$ est doublement périodique, ayant un infini double.

Maintenant, la condition

$$u = \varpi(x + y) - \theta(x - y)$$

donne

$$\frac{du}{dx} + \frac{du}{dy} = 2\varpi'(x + y),$$

et par conséquent

$$\frac{d^2u}{dx^2} - \frac{d^2u}{dy^2} = 0.$$

Or on a

$$\frac{du}{dx} = \frac{\psi'}{\varphi + \psi}\left(\frac{\varphi''}{\varphi + \psi} - 2\frac{\varphi'^2}{(\varphi + \psi)^2}\right).$$

Donc

$$\frac{d^2 u}{dx^2} = \frac{\psi'}{\varphi+\psi}\left[\frac{\varphi'''}{\varphi+\psi} - 6\,\frac{\varphi'\varphi''}{(\varphi+\psi)^2} + 6\,\frac{\varphi'^3}{(\varphi+\psi)^3}\right],$$

et, de même,

$$\frac{d^2 u}{dy^2} = \frac{\varphi'}{\varphi+\psi}\left[\frac{\psi'''}{\varphi+\psi} - 6\,\frac{\psi'\psi''}{(\varphi+\psi)^2} + 6\,\frac{\psi'^3}{(\varphi+\psi)^3}\right].$$

Egalons ces deux expressions, et divisons par $\frac{\varphi'\psi'}{(\varphi+\psi)^2}$ les deux membres de l'équation ainsi obtenue; il vient

$$(24)\qquad \frac{\varphi'''}{\varphi'} - 6\,\frac{\varphi''}{\varphi+\psi} + 6\,\frac{\varphi'^2}{(\varphi+\psi)^2} = \frac{\psi'''}{\psi'} - 6\,\frac{\psi''}{\varphi+\psi} + 6\,\frac{\psi'^2}{(\varphi+\psi)^2}.$$

En différentiant par rapport à $x$, on a

$$\frac{\varphi'\varphi^{\text{IV}} - \varphi''\varphi'''}{\varphi'^2} = 6\,\frac{\varphi'''}{\varphi+\psi} - 6\,\frac{\varphi''\varphi'}{(\varphi+\psi)^2} - 12\,\frac{\varphi'\varphi''}{(\varphi+\psi)^2} + 12\,\frac{\varphi'^3}{(\varphi+\psi)^3}$$
$$+ 6\,\frac{\varphi'\psi''}{(\varphi+\psi)^2} - 12\,\frac{\varphi'\psi'^2}{(\varphi+\psi)^3},$$

$$\frac{\varphi'\varphi^{\text{IV}} - \varphi''\varphi'''}{\varphi'^3} = 6\,\frac{\varphi'''}{\varphi'(\varphi+\psi)} - 18\,\frac{\varphi''}{(\varphi+\psi)^2} + 12\,\frac{\varphi'^2}{(\varphi+\psi)^3} + 6\,\frac{\psi''}{(\varphi+\psi)^2} - 12\,\frac{\psi'^2}{(\varphi+\psi)^3}.$$

Posons, pour abréger,

$$\frac{\varphi'\varphi^{\text{IV}} - \varphi''\varphi'''}{\varphi'^3} = z,$$

et différentions de nouveau par rapport à $x$ :

$$\frac{dz}{dx} = 6\,\frac{\varphi'\varphi^{\text{IV}} - \varphi''\varphi'''}{\varphi'^2(\varphi+\psi)} - 6\,\frac{\varphi'''}{(\varphi+\psi)^2} - 18\,\frac{\varphi'''}{(\varphi+\psi)^2} + 36\,\frac{\varphi'\varphi''}{(\varphi+\psi)^3} + 24\,\frac{\varphi'\varphi''}{(\varphi+\psi)^3}$$
$$- 36\,\frac{\varphi'^3}{(\varphi+\psi)^4} - 12\,\frac{\varphi'\psi''}{(\varphi+\psi)^3} + 36\,\frac{\varphi'\psi'^2}{(\varphi+\psi)^4}.$$

Substituons à $\frac{\varphi'\varphi^{\text{IV}}-\varphi''\varphi'''}{\varphi'^2}$ sa valeur trouvée ci-dessus :

$$\frac{dz}{dx} = 36\frac{\varphi'''}{(\varphi+\psi)^2} - 108\frac{\varphi'\varphi''}{(\varphi+\psi)^3} + 72\frac{\varphi'^3}{(\varphi+\psi)^4} + 36\frac{\varphi'\psi''}{(\varphi+\psi)^3} - 72\frac{\varphi'\psi'^2}{(\varphi+\psi)^4}$$
$$- 24\frac{\varphi'''}{(\varphi+\psi)^2} + 36\frac{\varphi'\varphi''}{(\varphi+\psi)^3} + 24\frac{\varphi'\varphi''}{(\varphi+\psi)^3} - 36\frac{\varphi'^3}{(\varphi+\psi)^4} - 12\frac{\varphi'\psi''}{(\varphi+\psi)^3}$$
$$+ 36\frac{\varphi'\psi'^2}{(\varphi+\psi)^4}.$$

Donc

$$\frac{dz}{dx} = 12\frac{\varphi'''}{(\varphi+\psi)^2} - 48\frac{\varphi'\varphi''}{(\varphi+\psi)^3} + 36\frac{\varphi'^3}{(\varphi+\psi)^4} + 24\frac{\varphi'\psi''}{(\varphi+\psi)^3} - 36\frac{\varphi'\psi'^2}{(\varphi+\psi)^4}.$$

Donc

$$z - \frac{\varphi}{\varphi'}\frac{dz}{dx} = 6\frac{\varphi''}{\varphi'(\varphi+\psi)} - 18\frac{\varphi''}{(\varphi+\psi)^2} + 12\frac{\varphi'^2}{(\varphi+\psi)^3} + 6\frac{\psi''}{(\varphi+\psi)^2} - 12\frac{\psi'^2}{(\varphi+\psi)^3}$$
$$- 12\frac{\varphi'''\varphi}{\varphi'(\varphi+\psi)^2} + 48\frac{\varphi''\varphi}{(\varphi+\psi)^3} - 36\frac{\varphi'^2\varphi}{(\varphi+\psi)^4} - 24\frac{\psi''\varphi}{(\varphi+\psi)^3} + 36\frac{\psi'^2\varphi}{(\varphi+\psi)^4},$$

d'où

$$z - \frac{\varphi}{\varphi'}\frac{dz}{dx} = -6\frac{\varphi'''}{\varphi'}\cdot\frac{\varphi-\psi}{(\varphi+\psi)^2} + 24\frac{\varphi''}{\varphi+\psi}\cdot\frac{\varphi-\psi}{(\varphi+\psi)^2} - 18\frac{\varphi'^2}{(\varphi+\psi)^2}\cdot\frac{\varphi-\psi}{(\varphi+\psi)^2}$$
$$- 12\frac{\psi''}{\varphi+\psi}\cdot\frac{\varphi-\psi}{(\varphi+\psi)^2} + 18\frac{\psi'^2}{(\varphi+\psi)^2}\cdot\frac{\varphi-\psi}{(\varphi+\psi)^2} + 6\frac{\varphi''-\psi''}{(\varphi+\psi)^2} - 6\frac{\varphi'^2-\psi'^2}{(\varphi+\psi)^3}.$$

Si l'on pose

$$\frac{\psi'\psi^{\text{IV}}-\psi''\psi'''}{\psi'^3} = t,$$

on aura

$$t - \frac{\psi}{\psi'}\frac{dt}{dy}$$

en changeant dans l'équation précédente $\varphi$ en $\psi$ et $\psi$ en $\varphi$. Ainsi

$$z - \frac{\varphi}{\varphi'}\frac{dz}{dx} = 6\frac{\varphi''-\psi''}{(\varphi+\psi)^2} - 6\frac{\varphi'^2-\psi'^2}{(\varphi+\psi)^3} - 6\frac{\varphi-\psi}{(\varphi+\psi)^2}\left[\frac{\varphi'''}{\varphi'} - 4\frac{\varphi''}{\varphi+\psi} + 3\frac{\varphi'^2}{(\varphi+\psi)^2}\right.$$
$$\left. + 2\frac{\psi''}{\varphi+\psi} - 3\frac{\psi'^2}{(\varphi+\psi)^2}\right].$$

et

$$t - \frac{\psi}{\psi'}\frac{dt}{dy} = -6\frac{\varphi'' - \psi''}{(\varphi+\psi)^2} + 6\frac{\varphi'^2 - \psi'^2}{(\varphi+\psi)^3} + 6\frac{\varphi-\psi}{(\varphi+\psi)^2}\left[\frac{\psi'''}{\psi'} - 4\frac{\psi''}{\varphi+\psi} + 3\frac{\psi'^2}{(\varphi+\psi)^2} + 2\frac{\varphi''}{\varphi+\psi} - 3\frac{\varphi'^2}{(\varphi+\psi)^2}\right].$$

Donc, en ajoutant,

$$z - \frac{\varphi}{\varphi'}\frac{dz}{dx} + t - \frac{\psi}{\psi'}\frac{dt}{dy} = -6\frac{\varphi-\psi}{(\varphi+\psi)^2}\left[\frac{\varphi'''}{\varphi'} - 6\frac{\varphi''}{\varphi+\psi} + 6\frac{\varphi'^2}{(\varphi+\psi)^2} - \frac{\psi'''}{\psi'} + 6\frac{\psi''}{\varphi+\psi} - 6\frac{\psi'^2}{(\varphi+\psi)^2}\right].$$

Le second membre est nul, en vertu de l'équation (24); or $z$ et $\varphi$ ne dépendent que de $x$, $t$ et $\psi$ ne dépendent que de $y$; donc, si l'on désigne par $b$ une constante,

$$z - \frac{\varphi}{\varphi'}\frac{dz}{dx} = 3b, \quad t - \frac{\psi}{\psi'}\frac{dt}{dy} = -3b.$$

Si l'on intègre, il vient

$$\frac{z}{\varphi} = \frac{3b}{\varphi} + 12a, \quad \frac{\varphi'\varphi^{\text{IV}} - \varphi''\varphi'''}{\varphi'^2} = 3b\varphi' + 12a\varphi\varphi',$$

$$\frac{\varphi'''}{\varphi'} = 6a\varphi^2 + 3b\varphi + c, \quad \varphi'' = 2a\varphi^3 + \frac{3b}{2}\varphi^2 + c\varphi + \frac{d}{2},$$

et enfin

$$\varphi'^2 = a\varphi^4 + b\varphi^3 + c\varphi^2 + d\varphi + h.$$

On obtiendra de même

$$\psi'^2 = a_1\psi^4 - b\psi^3 + c_1\psi^2 + d_1\psi + h_1.$$

Substituons maintenant les expressions trouvées dans l'équation (24), après avoir chassé les dénominateurs de cette équation, ce qui donne

$$\psi'[\varphi'''(\varphi+\psi)^2 - 6\varphi'\varphi''(\varphi+\psi) + 6\varphi'^3] = \varphi'[\psi'''(\varphi+\psi)^2 - 6\psi'\psi''(\varphi+\psi) + 6\psi'^3];$$

quand on aura fait cette substitution, on pourra diviser tous les termes par $\varphi'\psi'$, et il restera

$$\begin{aligned}(6a\varphi^2+3b\varphi+c)(\varphi+\psi)^2-(12a\varphi^3+9b\varphi^2+6c\varphi+3d)(\varphi+\psi)\\+6a\varphi^4+6b\varphi^3+6c\varphi^2+6d\varphi+6h\\=(6a_1\psi^2-3b\psi+c_1)(\varphi+\psi)^2-(12a_1\psi^3-9b\psi^2+6c_1\psi+3d_1)(\varphi+\psi)\\+6a_1\psi^4-6b\psi^3+6c_1\psi^2+6d_1\psi+6h_1.\end{aligned}$$

Si l'on développe, il vient, toutes réductions faites,

$$\begin{aligned}6a\varphi^2\psi^2+c(\varphi^2+\psi^2)-4c\varphi\psi+3d(\varphi-\psi)+6h\\=6a_1\varphi^2\psi^2+c_1(\varphi^2+\psi^2)-4c_1\varphi\psi+3d_1(\psi-\varphi)+6h_1,\end{aligned}$$

ce qui exige qu'on ait

$$a=a_1,\quad c=c_1,\quad d=-d_1,\quad h=h_1.$$

Donc

$$\varphi'^2=a\varphi^4+b\varphi^3+c\varphi^2+d\varphi+h \quad\text{et}\quad \psi'^2=a\psi^4-b\psi^3+c\psi^2-d\psi+h.$$

La fonction $\varphi$ est déterminée par l'une des deux équations

$$\frac{d\varphi}{dx}=\sqrt{a\varphi^4+b\varphi^3+c\varphi^2+d\varphi+h}$$

et

$$\frac{d\varphi}{dx}=-\sqrt{a\varphi^4+b\varphi^3+c\varphi^2+d\varphi+h}.$$

Nous désignerons la première fonction par $\varphi(x)$, la seconde sera alors $\varphi(-x)$. La fonction $\psi$ aura pareillement deux valeurs, qui seront $-\varphi(y)$ et $-\varphi(-y)$. Nous pouvons supposer que la fonction $\varphi$ se réduit à zéro pour la valeur zéro de la variable; cette fonction est d'ailleurs une fonction doublement périodique, aux périodes $\omega$ et $\omega'$, et nous désignerons par M la somme constante des deux valeurs de la variable qui donnent à $\varphi$ la même valeur.

Nous savons que, les fonctions $\varphi$ et $\psi$ étant ainsi déterminées, $u$ est

égale à la somme de deux fonctions dépendant, l'une de $x+y$ seulement, l'autre de $x-y$ seulement, et nous avons vu que ces deux fonctions doivent être doublement périodiques, ayant un infini double, et leurs périodes étant évidemment les mêmes que celles de la fonction $\varphi$. Nous allons achever de déterminer ces fonctions.

La fonction $u$ peut avoir quatre valeurs :

$$\frac{-\varphi'(x)\varphi(y)}{[\varphi(x)-\varphi(y)]^2}, \quad \frac{\varphi'(x)\varphi'(-y)}{[\varphi(x)-\varphi(-y)]^2}, \quad \frac{\varphi'(-x)\varphi'(y)}{[\varphi(-x)-\varphi(y)]^2}, \quad \frac{-\varphi'(-x)\varphi'(-y)}{[\varphi(-x)-\varphi(-y)]^2}.$$

Soit

$$\frac{d\varpi}{d\alpha} = \sqrt{4\varpi^3 + A\varpi^2 + B\varpi + C} \quad \text{et} \quad \frac{d\theta}{d\beta} = \sqrt{4\theta^3 + A\theta^2 + B\theta + C},$$

de sorte que $\theta(\beta) = \varpi(\beta)$, et supposons que $\varpi$ se réduise à zéro pour la valeur zéro de la variable. Nous allons voir que si l'on pose

$$u = \varpi(x+y+m) - \varpi(x-y+m_1),$$

on peut, pour les quatre valeurs de $u$, déterminer $m$ et $m_1$, de telle sorte que cette équation soit vérifiée.

Soit d'abord

$$u = \frac{-\varphi'(x)\varphi'(y)}{[\varphi(x)-\varphi(y)]^2}.$$

Si l'on regarde $x$ comme seule variable, $u$ change de signe quand on remplace $x$ par $M-x$. Cette fonction a quatre zéros simples, qui sont ceux de $\varphi'(x)$, c'est-à-dire $\frac{M}{2}$, $\frac{M}{2}+\frac{\omega}{2}$, $\frac{M}{2}+\frac{\omega'}{2}$, $\frac{M}{2}+\frac{\omega+\omega'}{2}$, car les infinis de $\varphi$ donnent à la fonction une valeur finie. Elle a aussi deux infinis doubles, qui sont $x=y$ et $x=M-y$.

Si l'on regarde $y$ comme seule variable, $u$ change de signe quand on remplace $y$ par $M-y$. Ses zéros sont encore $\frac{M}{2}$, $\frac{M}{2}+\frac{\omega}{2}$, $\frac{M}{2}+\frac{\omega'}{2}$, et $\frac{M}{2}+\frac{\omega+\omega'}{2}$; ses infinis $y=x$ et $y=M-x$.

Si l'on considère maintenant la fonction

$$v = \varpi(x+y+m) - \varpi(x-y+m_1),$$

quand on y remplace $x$ par $\mathrm{M}-x$, on a

$$v=\varpi(y-x+\mathrm{M}+m)-\varpi(\mathrm{M}-x-y+m_1).$$

La fonction n'aura fait que changer de signe, si, N représentant la somme constante des deux valeurs de la variable qui donnent à $\varpi$ la même valeur, on a

$$\mathrm{M}+m+m_1=\mathrm{N}.$$

Quand on remplace $y$ par $\mathrm{M}-y$, on a

$$v=\varpi(\mathrm{M}+m+x-y)-\varpi(x+y-\mathrm{M}+m_1);$$

la fonction n'aura fait que changer de signe, si

$$\mathrm{M}+m-m_1=0.$$

De là on tire

$$m=\frac{\mathrm{N}}{2}-\mathrm{M} \quad \text{et} \quad m_1=\frac{\mathrm{N}}{2}.$$

Si l'on regarde dans $v$, $x$ comme seule variable, $v$ a quatre zéros donnés par la condition

$$x+y+m=\mathrm{N}-x+y-m_1+k\omega+k'\omega', \quad \text{ou} \quad 2x=\mathrm{M}+k\omega+k'\omega';$$

donc, abstraction faite des multiples des périodes, les zéros sont $\frac{\mathrm{M}}{2}$, $\frac{\mathrm{M}}{2}+\frac{\omega}{2}$, $\frac{\mathrm{M}}{2}+\frac{\omega'}{2}$, $\frac{\mathrm{M}}{2}+\frac{\omega+\omega'}{2}$.

Si l'on regarde $y$ comme seule variable, les zéros sont donnés par la condition

$$x+y+m=x-y+m_1+k\omega+k'\omega', \quad \text{ou} \quad 2y=\mathrm{M}+k\omega+k'\omega';$$

donc, en faisant abstraction des multiples des périodes, les zéros sont $\frac{\mathrm{M}}{2}$, $\frac{\mathrm{M}}{2}+\frac{\omega}{2}$; $\frac{\mathrm{M}}{2}+\frac{\omega'}{2}$ et $\frac{\mathrm{M}}{2}+\frac{\omega+\omega'}{2}$.

La fonction $v$ a deux infinis doubles, donnés par la condition

$$x+y+m=\frac{\mathrm{N}}{2}+k\omega+k'\omega', \quad \text{ou} \quad x-y+m_1=\frac{\mathrm{N}}{2}+k\omega+k'\omega'.$$

D'où, en remplaçant $m$ et $m_1$ par leur valeur,

$$x = \mathrm{M} - y \quad \text{et} \quad x = y.$$

Les fonctions $u$ et $v$ ayant les mêmes zéros et les mêmes infinis sont égales à un facteur constant près, que l'on peut toujours supposer égal à l'unité.

La seconde valeur de $u$ se déduit de la première, en changeant le signe, et remplaçant $y$ par $-y$ ; la troisième se déduit aussi de la première, en changeant le signe, et remplaçant $x$ par $-x$ ; enfin la quatrième s'en déduit aussi, en changeant $x$ en $-x$ et $y$ en $-y$. Donc, si, pour abréger, on pose

$$\mathrm{R} = \sqrt{a\varphi^4 + b\varphi^3 + c\varphi^2 + d\varphi + h},$$

et

$$\mathrm{S} = \sqrt{a\psi^4 - b\psi^3 + c\psi^2 - d\psi + h},$$

les quatre valeurs de $u$ seront déterminées par le tableau suivant :

1° $\dfrac{d\varphi}{dx} = \mathrm{R}, \quad \dfrac{d\psi}{dy} = -\mathrm{S}, \quad u = \varpi\left(x + y + \dfrac{\mathrm{N}}{2} - \mathrm{M}\right) - \varpi\left(x - y + \dfrac{\mathrm{N}}{2}\right);$

2° $\dfrac{d\varphi}{dx} = \mathrm{R}, \quad \dfrac{d\psi}{dy} = \mathrm{S}, \quad u = \varpi\left(x + y + \dfrac{\mathrm{N}}{2}\right) - \varpi\left(x - y + \dfrac{\mathrm{N}}{2} - \mathrm{M}\right);$

3° $\dfrac{d\varphi}{dx} = -\mathrm{R}, \quad \dfrac{d\psi}{dy} = -\mathrm{S}, \quad u = \varpi\left(x + y + \dfrac{\mathrm{N}}{2}\right) - \varpi\left(x - y + \dfrac{\mathrm{N}}{2} + \mathrm{M}\right);$

4° $\dfrac{d\varphi}{dx} = -\mathrm{R}, \quad \dfrac{d\psi}{dy} = \mathrm{S}, \quad u = \varpi\left(x + y + \dfrac{\mathrm{N}}{2} + \mathrm{M}\right) - \varpi\left(x - y + \dfrac{\mathrm{N}}{2}\right).$

La fonction $u_1$ sera déterminée par des équations de même forme. Mais pour que la différence $u_1 - u$ se réduise à une fonction de $x + y$, sans que $u_1$ et $u$ soient identiques, il faut évidemment que $u$ soit déterminée par la première ou la quatrième formule, et que $u_1$ le soit par l'une des formules correspondantes, les fonctions $\varpi$ étant les mêmes dans l'expression de $u$ et dans celles de $u_1$. Il faut donc, en définitive, et il suffit, que $\psi(y) = -\varphi(y)$, que $\psi_1(y) = -\varphi_1(y)$, et que $\varphi$ et $\varphi_1$ soient des fonctions doublement périodiques, aux mêmes périodes, ayant deux zéros et deux infinis.

Si ces conditions sont remplies, on aura, en désignant par $\varpi$ une fonction doublement périodique aux mêmes périodes que $\varphi$ et $\varphi_1$, se réduisant à zéro pour la valeur zéro de la variable, et ayant un infini double $\frac{N}{2}$, en désignant aussi par M la somme constante des valeurs de la variable qui donnent à $\varphi$ la même valeur, et par $M_1$ la quantité analogue pour $\varphi_1$, et supposant enfin que $\varphi$ et $\varphi_1$ se réduisent à zéro pour la valeur zéro de la variable :

$$\frac{\varphi'_1\psi'_1}{(\varphi_1+\psi_1)^2}-\frac{\varphi'\psi'}{(\varphi+\psi)^2}=\varpi\left(x+y+\frac{N}{2}-M_1\right)-\varpi\left(x+y+\frac{N}{2}-M\right).$$

Donc l'équation (3) sera vérifiée.

## VII.

Soit $\theta(x+y)$ une fonction doublement périodique, ayant les mêmes périodes que la fonction $\varpi$ considérée ci-dessus, et se réduisant à zéro pour $x+y=0$ et pour $x+y=M+M_1$. Il est facile de voir que les fonctions

$$\frac{-\theta'(x+y)}{[\theta(x+y)-\theta(M)]^2}\quad\text{et}\quad\varpi\left(x+y+\frac{N}{2}-M_1\right)-\varpi\left(x+y+\frac{N}{2}-M\right)$$

ont les mêmes zéros et les mêmes infinis. Donc, si A représente une constante,

$$\frac{\varphi'_1\psi'_1}{(\varphi_1+\psi_1)^2}-\frac{\varphi'\psi'}{(\varphi+\psi)^2}=\frac{-A\theta'(x+y)}{[\theta(x+y)-\theta(M)]^2}.$$

Si l'on intègre par rapport à $y$, il vient

$$\frac{\varphi'}{\varphi+\psi}-\frac{\varphi'_1}{\varphi_1+\psi_1}+\mathcal{F}_1(x)=\frac{A}{\theta(x+y)-\theta(M)}.$$

Si l'on intègre de nouveau par rapport à $x$, et si l'on désigne par $F(x+y)$ une intégrale du second membre, il vient

$$L(\varphi+\psi)-L(\varphi_1+\psi_1)+\mathcal{F}_2(x)+\mathcal{F}_3(y)=F(x+y)$$

ou

$$\frac{\varphi+\psi}{\varphi_1+\psi_1}\mathcal{F}_4(x)\mathcal{F}_5(y)=e^{F(x+y)}.$$

Cette équation nous montre que si les valeurs de $\varphi$, $\psi$, $\varphi_1$ et $\psi_1$ déterminées ci-dessus, et qui nous fournissent la solution la plus générale de l'équation (3), peuvent aussi, sans nouvelles restrictions, vérifier l'équation (2), il faut que la fonction de $x+y$ qui figure dans cette équation soit de la forme $e^{F(x+y)}$, $F(x+y)$ ayant pour dérivée une fonction doublement périodique, aux mêmes périodes que $\varphi$ et $\varphi_1$, et dont les infinis sont M et $M_1$. Nous allons voir que cette condition est suffisante.

Soit

$$e^{F(x+y)}=\frac{\varphi(x)-\varphi(y)}{\varphi_1(x)-\varphi_1(y)}\mathcal{F}_1(x)\mathcal{F}_2(y).$$

Les fonctions $\mathcal{F}_1$ et $\mathcal{F}_2$ se déterminent en remplaçant $x$ ou $y$ par des constantes $p$ et $q$; il vient

$$\begin{aligned}&e^{F(x+y)-F(x+q)-F(p+y)}\\&=\frac{\varphi(x)-\varphi(y)}{\varphi_1(x)-\varphi_1(y)}\cdot\frac{\varphi_1(x)-\varphi_1(q)}{\varphi(x)-\varphi(q)}\cdot\frac{\varphi_1(p)-\varphi_1(y)}{\varphi(p)-\varphi(y)}\cdot\frac{\varphi(p)-\varphi(q)}{\varphi_1(p)-\varphi_1(q)}e^{-F(p+q)}.\end{aligned}$$

Le second membre est une fonction doublement périodique, dont les périodes sont $\omega$ et $\omega'$; il en est de même du premier. En effet, la fonction $F'(x+y)$ étant doublement périodique aux mêmes périodes, on a

$$F(x+y+K\omega+K'\omega')=F(x+y)+KF(\omega)+K'F(\omega').$$

Si donc on remplace $x$ par $x+K\omega+K'\omega'$ et $y$ par $y+K_1\omega+K'_1\omega'$, l'exposant de $e$ devient

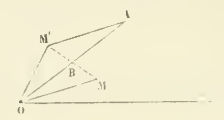
$$\begin{aligned}F(x+y)&+(K+K_1)F(\omega)+(K'+K'_1)F(\omega')-F(x+q)-KF(\omega)\\&-K'F(\omega')-F(y+p)-K_1F(\omega)-K'_1F(\omega'),\end{aligned}$$

ou

$$F(x+y)-F(x+q)-F(p+y).$$

Donc le premier membre, ne changeant pas quand on augmente $x$ et $y$ d'un multiple quelconque des périodes, est doublement périodique.

Le second membre a trois zéros, ce sont : $x = M - y$, $x = M_1 - q$, $y = M_1 - p$. Le premier membre admet les mêmes zéros et n'en admet pas d'autres. En effet, soit A le point qui correspond à la valeur $M + M_1$




de la variable; soient M et M' les points qui correspondent aux valeurs $z$ et $M + M_1 - z$ de cette variable; la droite MM' passe par le milieu B de OA, et la fonction F' prend la même valeur en deux points de OM et de AM' en ligne droite avec le point B, car la somme des valeurs de la variable correspondant à ces deux points est $M + M_1$. Or on peut former l'intégrale $F(M + M_1 - z)$ soit en parcourant la droite OM', soit en parcourant le contour OAM'. La droite OA donne $F(M + M_1)$; puisque F' passe par les mêmes valeurs quand on va de A en M' et quand on va de O en M, et que $dz$ a des signes contraires dans les deux cas, l'intégrale obtenue en allant de A en M' est $-F(z)$. Donc

$$F(M + M_1 - z) = F(M + M_1) - F(z).$$

Il en résulte que, F devenant infinie pour $z = M$ et pour $z = M_1$, la fonction $F(z)$ a des valeurs de signes contraires pour des valeurs de $z$ très-peu différentes de M et de $M_1$. Donc, si $F(M_1) = +\infty$,

$$F(M) = -\infty.$$

La fonction

$$e^{F(x+y) - F(x+q) - F(y+p)}$$

se réduit donc à zéro pour

$$x + y = M, \quad x + q = M_1 \quad \text{et} \quad p + y = M_1;$$

d'ailleurs F', et par conséquent F, n'a pas d'autres infinis; donc les zéros du premier membre sont les mêmes que ceux du second. On voit pareillement que les infinis sont aussi les mêmes; donc les deux fonctions sont égales à un facteur constant près.

Nous pouvons résumer ce qui précède en énonçant le théorème suivant :

*Pour que l'équation*

$$\mathfrak{F}(x+y) = \frac{F_1(x)f_2(y) + F_2(x)f_1(y)}{F_3(x)f_4(y) + F_4(x)f_3(y)}$$

*soit vérifiée, quelque valeur que l'on attribue aux variables $x$ et $y$, il faut et il suffit :*

1° *Que* $\frac{F_1(x)}{F_2(x)} = -\frac{f_1(x)}{f_2(x)}$ *et que* $\frac{F_3(x)}{F_4(x)} = -\frac{f_3(x)}{f_4(x)}$;

2° *Que ces fonctions* $\frac{F_1(x)}{F_2(x)}$, *etc., soient des fonctions doublement périodiques, aux mêmes périodes, ayant pour zéros, la première zéro et* M, *la seconde zéro et* $M_1$;

3° *Que* $\mathfrak{F}(x+y) = e^{F(x+y)}$, $F(x+y)$ *ayant pour dérivée une fonction doublement périodique aux mêmes périodes que les précédentes, et dont les infinis sont* M *et* $M_1$.

## VIII.

Considérons maintenant l'équation

$$(1) \qquad f(x+y) = \frac{\varphi'(x)\psi(y) + \varphi(x)\psi'(y)}{1 - K^2\varphi(x)^2\psi(y)^2}.$$

Cette équation peut se mettre sous la forme suivante

$$f(x+y) = \frac{\dfrac{\varphi(x)}{\varphi'(x)} + \dfrac{\psi(y)}{\psi'(y)}}{\dfrac{1}{\psi(y)^2} - K^2\varphi(x)^2}\,\frac{\varphi'(x)\psi'(y)}{\psi(y)^2}.$$

Pour qu'elle soit vérifiée, quelque valeur que l'on donne à $x$ et à $y$,

il faut d'abord que

$$\frac{\varphi(x)}{\varphi'(x)} = -\frac{\psi(x)}{\psi'(x)},$$

et que

$$\frac{1}{\psi(x)^2} = K^2\varphi(x)^2,$$

conditions équivalentes.

Il faut en outre que $\varphi(x)^2$ et $\frac{\varphi(x)}{\varphi'(x)}$ soient des fonctions doublement périodiques, aux mêmes périodes. Pour que $\varphi(x)^2$ soit doublement périodique, il faut que $\varphi(x)$ le soit également, et si $\omega$ et $\omega'$ sont les périodes de $\varphi$, celles de $\varphi^2$ seront $\frac{\omega}{2}$ et $\omega'$. Mais si $\varphi^2$ est nulle pour $x = 0$, elle l'est aussi pour $x = \frac{\omega}{2}$, donc $\varphi$ doit l'être pareillement. D'autre part, $\varphi^2$ reprenant la même valeur pour $x$ et pour $x + \frac{\omega}{2}$, $\varphi(x)$ doit être égale, soit à $\varphi\left(x + \frac{\omega}{2}\right)$, ce qui supposerait que les périodes de $\varphi$ sont $\omega'$ et $\frac{\omega}{2}$, contrairement à notre hypothèse, soit à $-\varphi\left(x + \frac{\omega}{2}\right)$. Mais la somme des zéros de $\varphi$ est $\frac{\omega}{2}$; donc

$$\varphi\left(x + \frac{\omega}{2}\right) = \varphi(-x);$$

donc

$$\varphi(x) = -\varphi(-x).$$

La fonction $\varphi$ est donc une fonction doublement périodique ayant deux zéros, et elle change seulement de signe quand la variable change de signe.

Cela étant, $\frac{\varphi}{\varphi'}$ est aussi doublement périodique aux périodes $\omega'$ et $\frac{\omega}{2}$. Elle se réduit à zéro quand $\varphi$ est nulle, c'est-à dire pour zéro et $\frac{\omega}{2}$, et quand $\varphi$ est infinie, c'est-à-dire pour $\frac{\omega'}{2}$ et $\frac{\omega + \omega'}{2}$. Donc la somme de ses zéros est $\frac{\omega'}{2}$.

$\varphi$ sera donc une fonction donnée par l'équation

$$\frac{d\varphi}{dx} = g\sqrt{(1-\varphi^2)(1-k^2\varphi^2)},$$

$g$ et $k$ étant deux paramètres arbitraires, $\varphi$ se réduisant à zéro pour $x = 0$, et la valeur correspondante du radical étant $1$. Quant à $\psi(y)$, elle sera donnée par l'équation

$$\psi(y) = m\varphi\left(\frac{\omega'}{2} + y\right),$$

$m$ étant une constante déterminée par la condition $m^2 = \frac{k^2}{K^2}$; car $\frac{1}{\psi(y)} = \frac{1}{m\varphi\left(\frac{\omega'}{2}+y\right)} = \frac{k\varphi(y)}{m}$; donc pour que $\frac{1}{\psi(y)^2} = \varphi(y)^2 K^2$, il faut que $\frac{k^2}{m^2} = K^2$.

Soit maintenant $f(x+y) = e^{F(x+y)}$, d'où $F' = \frac{f'}{f}$. Nous savons que $F'$ doit être une fonction doublement périodique, ayant les mêmes périodes que $\varphi^2$ et $\frac{\varphi}{\varphi'}$, et devenant infinie pour les valeurs zéro et $\frac{\omega'}{2}$ de la variable. Cette condition sera remplie si l'on a

$$f(x+y) = \varphi\left(x+y+\frac{\omega'}{2}\right).$$

Il est facile en effet de vérifier que, si l'on représente par $\varphi$ une fonction elliptique, déterminée comme il a été dit ci-dessus, on a toujours

$$\varphi\left(x+y+\frac{\omega'}{2}\right) = m\,\frac{\varphi(x)\varphi'\left(y+\frac{\omega'}{2}\right)+\varphi\left(y+\frac{\omega'}{2}\right)\varphi'(x)}{1-k^2\varphi(x)^2\varphi\left(y+\frac{\omega'}{2}\right)^2}.$$

Les zéros des deux membres, dans chaque parallélogramme élémentaire, sont

$$x = -\left(y+\frac{\omega'}{2}\right) \quad \text{et} \quad x = \frac{\omega}{2} - \left(y+\frac{\omega'}{2}\right),$$

et les infinis sont

$$x + y = 0 \quad \text{et} \quad x + y + \frac{\omega'}{2} = \frac{\omega}{2} + \frac{\omega'}{2}.$$

## IX.

Il nous reste à considérer l'équation

$$(1) \qquad \frac{\mathcal{F}(x+y)}{\mathcal{F}_1(x-y)} = \frac{F(x)f_1(y) + f(x)F_1(y)}{F(x)f_1(y) - f(x)F_1(y)}.$$

Soit

$$\frac{F(x)}{f(x)} = \varphi(x) \quad \text{et} \quad \frac{F_1(y)}{f_1(y)} = \psi(y),$$

d'où

$$(2) \qquad \frac{\mathcal{F}(x+y)}{\mathcal{F}_1(x-y)} = \frac{\varphi+\psi}{\varphi-\psi} \quad \text{ou} \quad \mathcal{F}(\varphi-\psi) = \mathcal{F}_1(\varphi+\psi).$$

En différentiant par rapport à $x$ et par rapport à $y$, on a

$$\mathcal{F}'(\varphi-\psi) + \mathcal{F}\varphi' = \mathcal{F}'_1(\varphi+\psi) + \mathcal{F}_1\varphi',$$
$$\mathcal{F}'(\varphi-\psi) - \mathcal{F}\psi' = -\mathcal{F}'_1(\varphi+\psi) + \mathcal{F}_1\psi'.$$

Nous éliminerons $\mathcal{F}'_1$ entre ces deux équations en les ajoutant :

$$2\mathcal{F}'(\varphi-\psi) + \mathcal{F}(\varphi'-\psi') = \mathcal{F}_1(\varphi'+\psi').$$

Si l'on élimine maintenant $\mathcal{F}_1$ au moyen de l'équation (2), on a

$$2\mathcal{F}'(\varphi^2-\psi^2) + \mathcal{F}(\varphi'-\psi')(\varphi+\psi) = \mathcal{F}(\varphi-\psi)(\varphi'+\psi'),$$

$$(3) \qquad \frac{\mathcal{F}'}{\mathcal{F}} = \frac{\varphi\psi'-\psi\varphi'}{\varphi^2-\psi^2}.$$

Cette équation est de même forme que celles que nous venons d'étudier ; elle détermine pour $\varphi$ une fonction elliptique, définie, comme ci-dessus, par l'équation

$$\frac{d\varphi}{dx} = g\sqrt{(1-\varphi^2)(1-k^2\varphi^2)},$$

et l'on doit avoir

$$\psi(y) = \varphi(y).$$

La fonction $\frac{\mathfrak{F}'}{\mathfrak{F}}$ doit être une fonction elliptique, impaire, ayant pour périodes $\omega$ et $\omega'$; cette condition sera remplie si $\mathfrak{F}$ est une fonction elliptique, impaire, ayant pour périodes $\omega$ et $2\omega'$, s'annulant pour les valeurs zéro et $\omega'$, et devenant infinie pour les valeurs $\frac{\omega}{2}$ et $\omega' + \frac{\omega}{2}$ de la variable. Il est facile en effet de vérifier que, s'il en est ainsi, les fonctions

$$\frac{\mathfrak{F}(x+y)}{\mathfrak{F}(x-y)} \quad \text{et} \quad \frac{\varphi(x)+\varphi(y)}{\varphi(x)-\varphi(y)}$$

ont les mêmes zéros et les mêmes infinis. Les zéros sont

$$x = -y \quad \text{et} \quad x = \frac{\omega}{2} + y;$$

les infinis sont

$$x = y \quad \text{et} \quad x = \frac{\omega}{2} - y.$$

# NOTE

SUR UNE

# FORMULE PROPRE A FACILITER LE DÉVELOPPEMENT DE LA FONCTION PERTURBATRICE;

PAR M. V. PUISEUX.

La fonction perturbatrice correspondante à l'action mutuelle de deux planètes se compose de deux parties dont la plus importante a pour dénominateur la distance mutuelle des deux astres. Quand on développe cette fonction à la manière ordinaire, chaque terme provenant de la partie principale renferme les demi grands axes $a$ et $a'$ des deux orbites dans un facteur de la forme

$$a^p a'^{p'} \frac{d^{p+p'}\left(a^k a'^k B_{k+\frac{1}{2}}^{(i)}\right)}{da^p\, da'^{p'}},$$

où la quantité $B_{k+\frac{1}{2}}^{(i)}$ est définie par l'équation

$$(a^2+a'^2-2aa'\cos\theta)^{-k-\frac{1}{2}} = \frac{1}{2} B_{k+\frac{1}{2}}^{(0)} + B_{k+\frac{1}{2}}^{(1)}\cos\theta + B_{k+\frac{1}{2}}^{(2)}\cos 2\theta + \ldots.$$

Le facteur dont on vient de parler peut être regardé comme une fonction homogène, du degré $-1$, des deux variables $a$ et $a'$. Pour faciliter les réductions, il convient de l'exprimer au moyen d'une fonction d'une seule variable et de ses dérivées successives. Pour cela

on pose ($a'$ désignant la plus petite des deux quantités $a$, $a'$)

$$\frac{a'}{a} = \alpha,$$

$$(1 + \alpha^2 - 2\alpha\cos\theta)^{-k-\frac{1}{2}} = \frac{1}{2} b^{(0)}_{k+\frac{1}{2}} + b^{(1)}_{k+\frac{1}{2}}\cos\theta + b^{(2)}_{k+\frac{1}{2}}\cos 2\theta + \ldots,$$

en sorte que $b^{(i)}_{k+\frac{1}{2}}$ soit une fonction de la seule variable $\alpha$.

On a alors la relation

$$a^k a'^k \mathrm{B}^{(i)}_{k+\frac{1}{2}} = \frac{1}{a}\alpha^k b^{(i)}_{k+\frac{1}{2}};$$

en la différentiant successivement, on en déduit de proche en proche les valeurs des diverses dérivées partielles $\dfrac{d^{p+p'}\left(a^k a'^k \mathrm{B}^{(i)}_{k+\frac{1}{2}}\right)}{da^p\, da'^{p'}}$ en fonction de $b^{(i)}_{k+\frac{1}{2}}$, $\dfrac{db^{(i)}_{k+\frac{1}{2}}}{d\alpha}$, $\dfrac{d^2 b^{(i)}_{k+\frac{1}{2}}}{d\alpha^2}$, etc. Mais on peut aussi former directement l'expression de chacune de ces dérivées à l'aide d'une formule qu'il me paraît utile de signaler. Cette formule peut s'écrire

$$a^p a'^{p'} \frac{d^{p+p'}\left(a^k a'^k \mathrm{B}^{(i)}_{k+\frac{1}{2}}\right)}{da^p\, da'^{p'}}$$

$$= \frac{(-1)^p \alpha^k}{a} \times \left\{ \begin{array}{l} \alpha^{p+p'} \dfrac{d^{p+p'} b^{(i)}_{k+\frac{1}{2}}}{d\alpha^{p+p'}} + \dfrac{p+k}{1}(p+p')\,\alpha^{p+p'-1} \dfrac{d^{p+p'-1} b^{(i)}_{k+\frac{1}{2}}}{d\alpha^{p+p'-1}} \\ + \dfrac{(p+k)(p+k-1)}{1.2}(p+p')(p+p'-1)\,\alpha^{p+p'-2} \dfrac{d^{p+p'-2} b^{(i)}_{k+\frac{1}{2}}}{d\alpha^{p+p'-2}} + \ldots \end{array} \right\}.$$

J'indiquerai encore à cette occasion l'équation suivante

$$a^p a'^{p'} \frac{d^{p+p'} \mathrm{B}^{(i)}_{k+\frac{1}{2}}}{da^p\, da'^{p'}}$$

$$= \frac{(-1)^p}{a^{2k+1}} \times \left\{ \begin{array}{l} \alpha^{p+p'} \dfrac{d^{p+p'} b^{(i)}_{k+\frac{1}{2}}}{d\alpha^{p+p'}} + \dfrac{p}{1}(p+p'+2k)\,\alpha^{p+p'-1} \dfrac{d^{p+p'-1} b^{(i)}_{k+\frac{1}{2}}}{d\alpha^{p+p'-1}} \\ + \dfrac{p(p-1)}{1.2}(p+p'+2k)(p+p'+2k-1)\,\alpha^{p+p'-2} \dfrac{d^{p+p'-2} b^{(i)}_{k+\frac{1}{2}}}{d\alpha^{p+p'-2}} + \ldots \end{array} \right\}.$$

Dans ces formules, les nombres entiers positifs $p$, $p'$ peuvent se réduire à zéro; $k$ peut être un nombre fractionnaire quelconque positif ou négatif. On les vérifiera aisément en supposant qu'elles soient vraies pour des valeurs de $p$ et de $p'$ respectivement inférieures à de certaines limites, et démontrant qu'elles subsistent encore lorsqu'on augmente l'une ou l'autre limite d'une unité.

Les deux équations précédentes sont comprises d'ailleurs dans une formule plus générale que je me dispense de transcrire ici et qui sert à exprimer en fonction de $\alpha$, $u$, $\frac{du}{d\alpha}$, $\frac{d^2 u}{d\alpha^2}$, etc., la quantité

$$a^{p-q} a'^{p'-q'} \frac{d^{p+p'}(a^q a'^{q'} u)}{da^p\, da'^{p'}},$$

où $u$ désigne une fonction quelconque du rapport $\alpha = \frac{a}{a'}$, les nombres $q$, $q'$ pouvant être entiers ou fractionnaires, positifs ou négatifs.

# NOUVEAUX THÉORÈMES

CONCERNANT

## LES FONCTIONS $N(n, p, q)$ ET D'AUTRES FONCTIONS QUI S'Y RATTACHENT;

**Par M. J. LIOUVILLE.**

---

1. Je désigne par $N(n, p, q)$ le nombre des décompositions d'un entier donné $n$ en $p$ carrés dont les $q$ premiers sont impairs et à racines positives, tandis que les $(p-q)$ derniers sont pairs et à racines indifféremment positives, nulles ou négatives. Cette notation a déjà été employée dans le cahier de juillet, où j'ai communiqué deux théorèmes en prenant pour $n$ un nombre impairement pair. Ici au contraire je supposerai $n$ pairement pair, savoir

$$n = 2^{\alpha+2} m,$$

$m$ étant impair et $\alpha$ pouvant se réduire à zéro, mais n'étant jamais négatif. Il y a pour ces nombres pairement pairs deux théorèmes tout à fait analogues à ceux que j'ai donnés pour les nombres impairement pairs: on y verra figurer de nouveau les fonctions $\zeta_\mu(m)$, $\rho_\mu(m)$ que je définis, comme on sait, par les équations

$$\zeta_\mu(m) = \sum d^\mu, \quad \rho_\mu(m) = \sum (-1)^{\frac{\delta-1}{2}} d^\mu,$$

dans lesquelles le signe sommatoire porte sur les groupes de diviseurs conjugués $d$, $\delta$ du nombre $m = d\delta$.

*Théorème I.* — « Soit $\nu$ un entier donné $> 0$ : je dis qu'il existe » des constantes $a_0, a_1, a_2, \ldots, a_{\nu-1}$ telles, que l'on puisse poser, pour » tout entier impair $m$ et pour tout entier $\alpha$ positif ou nul, l'équa-

tion

$$2^{(2\nu+1)\alpha}\zeta_{2\nu+1}(m) = \sum a_s \mathrm{N}(2^{\alpha+2}m, 4\nu+4, 4s+4),$$

» le signe $\sum$ portant sur $s$ dont les valeurs sont 0, 1, 2,..., $\nu - 1$. »

Les coefficients $a_0, a_1, a_2, \ldots, a_{\nu-1}$ sont constants en ce sens qu'ils ne dépendent ni de $m$, ni de $\alpha$; mais ils changent quand $\nu$ change. Cependant on a toujours $a_0 = 1$. On a aussi $a_{\nu-1} = 16^{\nu-1}$, et en général

$$a_{\nu-s-1} = 16^{\nu-2s-1}a_s.$$

Au reste les coefficients $a_s$ se déterminent aisément, pour chaque valeur donnée de $\nu$, au moyen des plus petites valeurs de $2^{\alpha+2}m$.

Pour la plus petite valeur de $\nu$, c'est-à-dire pour $\nu = 1$, on a

$$2^{3\alpha}\zeta_3(m) = \mathrm{N}(2^{\alpha+2}m, 8, 4).$$

Pour $\nu = 2$, il vient

$$2^{5\alpha}\zeta_5(m) = \mathrm{N}(2^{\alpha+2}m, 12, 4) + 16\,\mathrm{N}(2^{\alpha+2}m, 12, 8).$$

Pour $\nu = 3$, je trouve

$$2^{7\alpha}\zeta_7(m) = \mathrm{N}(2^{\alpha+2}m, 16, 4) + 104\,\mathrm{N}(2^{\alpha+2}m, 16, 8) + 256\,\mathrm{N}(2^{\alpha+2}m, 16, 12).$$

Et ainsi de suite. On voit que ces équations ne commencent qu'à $\zeta_3(m)$ : il n'y en a pas cette fois pour $\zeta_1(m)$.

*Théorème II.* — « Soit $\nu$ un entier donné $> 0$ : je dis qu'il existe » des constantes $b_0, b_1, b_2, \ldots, b_{\nu-1}$ telles, que l'on puisse poser, pour » tout entier impair $m$ et pour tout entier $\alpha$ positif ou nul, l'équation

$$2^{2\alpha\nu}\rho_{2\nu}(m) = \sum b_s \mathrm{N}(2^{\alpha+2}m, 4\nu+2, 4s+4),$$

» le signe $\sum$ portant sur $s$ dont les valeurs sont 0, 1, 2,..., $\nu - 1$. »

Les coefficients $b_s$ sont constants en ce sens qu'ils ne dépendent ni de $m$, ni de $\alpha$; mais ils changent quand $\nu$ change : cependant on a toujours $b_0 = 1$. Au reste ces coefficients $b_s$ se déterminent facilement, pour chaque valeur donnée de $\nu$, au moyen des plus petites valeurs de $2^{\alpha+2}m$.

Pour $\nu = 1$, on a

$$2^{2\alpha}\rho_2(m) = \text{N}(2^{\alpha+2}m, 6, 4).$$

Pour $\nu = 2$, il vient

$$2^{4\alpha}\rho_4(m) = \text{N}(2^{\alpha+2}m, 10, 4) + 4\text{N}(2^{\alpha+2}m, 10, 8).$$

Pour $\nu = 3$, je trouve

$$2^{6\alpha}\rho_6(m) = \text{N}(2^{\alpha+2}m, 14, 4) + 44\text{N}(2^{\alpha+2}m, 14, 8) + 16\text{N}(2^{\alpha+2}m, 14, 12).$$

Et ainsi de suite. On voit qu'on ne commence qu'à $\rho_2(m)$, et qu'il n'y a pas d'équation relative à $\rho(m)$.

2. Nous réservons pour un autre moment les applications qu'on peut faire de ces formules, déjà très-curieuses par elles-mêmes. Mais il nous est impossible de ne pas indiquer ici quelques conséquences qu'on en déduit immédiatement en les comparant entre elles pour diverses valeurs de $\alpha$, ou bien en les comparant à celles qu'on a données dans le cahier de juillet au sujet des nombres impairement pairs. Il suffira en effet d'éliminer les fonctions $\zeta$ ou les fonctions $\rho$ pour avoir des relations simples (et partant dignes d'intérêt) entre les seules fonctions N.

Prenez, par exemple, dans le cahier de juillet, l'équation

$$\zeta_5(m) = \text{N}(2m, 12, 2) + 224\text{N}(2m, 12, 6) + 256\text{N}(2m, 12, 10)$$

et rapprochez-la de l'équation

$$2^{5\alpha}\zeta_5(m) = \mathrm{N}(2^{\alpha+2}m, 12, 4) + 16\mathrm{N}(2^{\alpha+2}m, 12, 8):$$

vous en conclurez que, quels que soient $m$ et $\alpha$, les deux quantités

$$\mathrm{N}(2^{\alpha+2}m, 12, 4) + 16\mathrm{N}(2^{\alpha+2}m, 12, 8)$$

et

$$2^{5\alpha}[\mathrm{N}(2m, 12, 2) + 224\mathrm{N}(2m, 12, 6) + 256\mathrm{N}(2m, 12, 10)]$$

sont égales entre elles.

De même on n'a qu'à comparer les équations

$$\rho_4(m) = \mathrm{N}(2m, 10, 2) + 64\mathrm{N}(2m, 10, 6)$$

et

$$2^{4\alpha}\rho_4(m) = \mathrm{N}(2^{\alpha+2}m, 10, 4) + 4\mathrm{N}(2^{\alpha+2}m, 10, 8),$$

pour en conclure que les deux expressions

$$\mathrm{N}(2^{\alpha+2}m, 10, 4) + 4\mathrm{N}(2^{\alpha+2}m, 10, 8)$$

et

$$2^{4\alpha}[\mathrm{N}(2m, 10, 2) + 64\mathrm{N}(2m, 10, 6)$$

sont toujours égales.

On nous dispensera d'écrire sous leur forme générale les équations auxquelles ces considérations conduisent.

5. Nous avons désigné par $\mathrm{N}(n, p, q)$ le nombre total des solutions tant propres qu'impropres de l'équation

$$n = i_1^2 + \ldots + i_q^2 + \varpi_1^2 + \ldots + \varpi_{p-q}^2,$$

où (nous le répétons) les entiers $i$ sont impairs et positifs, tandis que les entiers $\varpi$ sont pairs et indifféremment positifs, nuls ou négatifs. On pourrait aussi considérer à part le nombre des solutions propres, c'est-à-dire des solutions pour lesquelles aucun entier $> 1$ ne divise à

la fois $i_1, \ldots, i_q, \varpi_1, \ldots, \varpi_{p-q}$. Désignons ce nombre par

$$M(n, p, q),$$

et nous aurons pour la fonction M des théorèmes tout à fait analogues à ceux que nous venons de donner pour la fonction N. Il n'y a qu'à substituer dans nos formules aux fonctions $\zeta_\mu(m)$, $\rho_\mu(m)$ d'autres fonctions que je vais définir et dont l'une du reste s'est déjà dans le temps présentée à nous.

Soit P un quelconque des diviseurs premiers de l'entier impair donné $m$, et $r$ son exposant dans $m$ de façon qu'on puisse écrire, d'après une notation connue,

$$m = \prod (P^r),$$

puis faisons

$$Z_\mu(m) = \prod [P^{r\mu} + P^{(r-1)\mu}]$$

et

$$R_\mu(m) = \prod \left[P^{r\mu} + (-1)^{\frac{P-1}{2}} P^{(r-1)\mu}\right].$$

C'est la fonction

$$Z_\mu(m)$$

qui devra remplacer

$$\zeta_\mu(m),$$

et la fonction

$$R_\mu(m)$$

remplacera

$$\rho_\mu(m).$$

On aura donc

$$Z_{2\nu-1}(m) = \sum A_s M(2m, 4\nu, 4s+2),$$

le signe sommatoire portant sur $s$ dont les valeurs successives sont $0$, $1$, $2, \ldots, \nu-1$, et les coefficients $A_s$ étant, pour chaque valeur du

nombre entier positif $\nu$, les mêmes que dans la formule

$$\zeta_{2\nu-1}(m) = \sum A_s N(2m, 4\nu, 4s+2)$$

du cahier de juillet.

Avec les coefficients $B_s$ de la formule

$$\rho_{2\nu}(m) = \sum B_s N(2m, 4\nu+2, 4s+2),$$

on aura semblablement

$$R_{2\nu}(m) = \sum B_s M(2m, 4\nu+2, 4s+2);$$

ici on peut avoir $\nu = 0$, et les valeurs de $s$ sont $0, 1, 2, 3, \ldots, \nu-1, \nu$; mais $B_\nu = 0$ dès que $\nu$ est $> 0$.

Aux formules nouvelles données dans le présent article pour les fonctions N répondront de même des formules concernant les fonctions M où figureront les coefficients $a_s$, $b_s$.

Ainsi l'on aura

$$2^{(2\nu+1)\alpha} Z_{2\nu+1}(m) = \sum a_s M(2^{\alpha+2} m, 4\nu+4, 4s+4):$$

l'entier $\nu$ est $> 0$; le signe sommatoire porte sur $s$ dont les valeurs successives sont $0, 1, 2, \ldots, \nu-1$.

On aura pareillement

$$2^{2\alpha\nu} R_{2\nu}(m) = \sum b_s M(2^{\alpha+2} m, 4\nu+2, 4s+4)$$

avec les mêmes conditions pour $\nu$ et $s$.

Restent les équations entre les seules fonctions N. Celles-là, bien évidemment, s'appliqueront d'elles-mêmes aux fonctions M sans qu'on ait rien à y changer.

Ainsi, par exemple, de l'égalité des deux quantités

$$N(2^{\alpha+2} m, 12, 4) + 16 N(2^{\alpha+2} m, 12, 8)$$

et

$$2^{5\alpha}[\mathrm{N}(2m, 12, 2) + 224\mathrm{N}(2m, 12, 6) + 256\mathrm{N}(2m, 12, 10)],$$

on conclura que ces deux autres quantités

$$\mathrm{M}(2^{\alpha+2}m, 12, 4) + 16\mathrm{M}(2^{\alpha+2}m, 12, 8)$$

et

$$2^{5\alpha}[\mathrm{M}(2m, 12, 2) + 224\mathrm{M}(2m, 12, 6) + 256\mathrm{M}(2m, 12, 10)$$

sont aussi égales.

Semblablement, de l'égalité des deux expressions

$$\mathrm{N}(2^{\alpha+2}m, 10, 4) + 4\mathrm{N}(2^{\alpha+2}m, 10, 8)$$

et

$$2^{4\alpha}[\mathrm{N}(2m, 10, 2) + 64\mathrm{N}(2m, 10, 6)],$$

on conclura que ces deux autres expressions

$$\mathrm{M}(2^{\alpha+2}m, 10, 4) + 4m(2^{\alpha+2}m, 10, 8)$$

et

$$2^{4\alpha}[\mathrm{M}(2m, 10, 2) + 64\mathrm{M}(2m, 10, 6)]$$

sont égales entre elles.

4. Il ne sera pas inutile, en terminant, de rappeler comment les fonctions $\mathrm{Z}_\mu(m)$ sont liées aux fonctions $\zeta_\mu(m)$; car les fonctions $\mathrm{R}_\mu(m)$ sont liées de la même manière aux fonctions $\rho_\mu(m)$. Considérons spécialement, parmi les diviseurs de $m$, ceux qui s'expriment par un carré $\mathrm{D}^2$. L'unité est toujours un tel diviseur, mais il peut y en avoir d'autres. Or on a

$$\sum \mathrm{Z}_\mu\left(\frac{m}{\mathrm{D}^2}\right) = \zeta_\mu(m)$$

et

$$\sum \mathrm{R}_\mu\left(\frac{m}{\mathrm{D}^2}\right) = \rho_\mu(m),$$

le signe $\sum$ portant sur tous les diviseurs $D^2$. J'ajouterai que l'on a pareillement

$$\sum M\left(\frac{2m}{D^2}, p, q\right) = N(2m, p, q).$$

On a même encore

$$\sum M\left(\frac{2^{\alpha+2}m}{D^2}, p, q\right) = N(2^{\alpha+2}m, p, q),$$

mais cette dernière fois sous la condition essentielle de $q > 0$.

# NOUVELLE THÉORIE
DES
# FONCTIONS DE VARIABLES IMAGINAIRES;

PAR M. MAXIMILIEN MARIE,
Ancien élève de l'École Polytechnique.

## QUATRIÈME PARTIE.
DES ANGLES IMAGINAIRES ET DE LA COURBURE DES COURBES ET SURFACES IMAGINAIRES.

## CHAPITRE IX.
*De la courbure des courbes imaginaires.*

**133.** *Des contacts des divers ordres des lieux plans en général.* — Deux courbes réelles,

$$f(x, y) = 0 \quad \text{et} \quad f_1(x, y) = 0,$$

qui passent en un même point réel $[x, y]$, ont en ce point un contact de l'ordre $n$, lorsque $\frac{dy}{dx}, \frac{d^2y}{dx^2}, \ldots, \frac{d^ny}{dx^n}$, tirées des deux équations séparément, y ont les mêmes valeurs.

On serait disposé à appliquer, sans nouvelle démonstration, le même principe aux courbes imaginaires : cependant, outre que l'énoncé doit en être complété alors par une restriction spéciale destinée à faire connaître expressément les lieux conjoints auxquels le théorème est applicable, la vérification en est en quelque sorte rendue nécessaire par la composition des coordonnées en parties réelles et imaginaires,

et par l'obscurité qui s'attache en conséquence à la notion même des coefficients différentiels $\frac{dy}{dx}$, $\frac{d^2y}{dx^2}$, etc.

Nous croyons donc devoir établir directement le théorème suivant :

Si deux équations

$$f(x, y) = 0, \quad f_1(x, y) = 0,$$

ont une solution commune, réelle ou imaginaire, $[x, y]$, et qu'au point correspondant, $\frac{dy}{dx}$, $\frac{d^2y}{dx^2}$, ..., $\frac{d^ny}{dx^n}$, tirées séparément des deux équations, présentent les mêmes valeurs, les lieux partant du point $[x, y]$, qui seraient définis par les équations

$$f(x, y) = 0 \quad \text{ou} \quad f_1(x, y) = 0$$

et par une relation complémentaire commune, $\varphi(\alpha, \beta) = 0$, établie entre les parties réelle et imaginaire de $x$, auront au point $[x, y]$ un contact de l'ordre $n$, c'est-à-dire que $x_1$ et $y_1$ désignant les coordonnées réelles de l'un ou de l'autre des deux lieux, $\frac{dy_1}{dx_1}$, $\frac{d^2y_1}{dx_1^2}$, ..., $\frac{d^ny_1}{(dx_1)^n}$, auront les mêmes valeurs de part et d'autre au point commun à ces deux lieux.

Il suffira pour cela d'établir que

$$\frac{dx_1}{d\alpha}, \frac{d^2x_1}{d\alpha^2}, \dots, \frac{d^nx_1}{d\alpha^n}$$

et

$$\frac{dy_1}{d\alpha}, \frac{d^2y_1}{d\alpha^2}, \dots, \frac{d^ny_1}{d\alpha^n}$$

auront les memes valeurs de part et d'autre; car $\frac{dy_1}{dx_1}$, $\frac{d^2y_1}{dx_1^2}$, ..., $\frac{d^ny_1}{dx_1^n}$, dépendant de

$$\frac{dx_1}{d\alpha}, \frac{d^2x_1}{d\alpha^2}, \dots, \frac{d^nx_1}{d\alpha^n}$$

et de

$$\frac{dy_1}{d\alpha}, \frac{d^2y_1}{d\alpha^2}, \dots, \frac{d^ny_1}{d\alpha^n}$$

auront par suite aussi les mêmes valeurs de part et d'autre.

Or la loi de progression de $x_1$ étant de part et d'autre réglée par les mêmes équations

$$x_1 = \alpha + \beta,$$

$$\varphi(\alpha, \beta) = 0,$$

les dérivées de tous les ordres de $x_1$, par rapport à $\alpha$, seront d'elles-mêmes égales de part et d'autre; de sorte que la démonstration doit porter seulement sur les dérivées de $y_1$ par rapport à $\alpha$.

Mais les dérivées de $y_1$, par rapport à $\alpha$, se déduisant de celles de $y$, par rapport à la même variable, en y remplaçant $\sqrt{-1}$ par $1$, tout se réduira, en définitive, à établir l'identité des valeurs de

$$\frac{dy}{d\alpha}, \quad \frac{d^2y}{d\alpha^2}, \ldots, \quad \frac{d^ny}{d\alpha^n},$$

tirées séparément des deux équations proposées.

Or

$$\frac{dy}{d\alpha} = \frac{dy}{dx}\left(1 + \frac{d\beta}{d\alpha}\sqrt{-1}\right),$$

$$\frac{d^2y}{d\alpha^2} = \frac{d^2y}{dx^2}\left(1 + \frac{d\beta}{d\alpha}\sqrt{-1}\right)^2 + \frac{dy}{dx}\frac{d^2\beta}{d\alpha^2}\sqrt{-1},$$

. . . . . . . . . . . . . . . . . . . . . . .

Ces équations montrent suffisamment que les dérivées de $y$, par rapport à $\alpha$, ne dépendant que de celles de $y$ par rapport à $x$, qui sont supposées égales de part et d'autre, et de celles de $\beta$ par rapport à $\alpha$, qui sont identiques, seront aussi égales.

On pourrait évidemment substituer à la relation $\varphi(\alpha, \beta) = 0$ une équation quelconque entre $\alpha$, $\beta$, $\alpha'$ et $\beta'$ : mais la démonstration du théorème montre même qu'à une relation commune $\varphi(\alpha, \beta) = 0$, on pourrait substituer deux relations différentes $\psi(\alpha, \beta) = 0$, $\chi(\alpha, \beta) = 0$ qui donnassent au point $[x, y]$ les mêmes valeurs pour

$$\frac{d\beta}{d\alpha}, \quad \frac{d^2\beta}{d\alpha^2}, \ldots, \quad \frac{d^n\beta}{d\alpha^n}.$$

**134.** *Des contacts des divers ordres des conjuguées, de même ca-*

*ractéristique, de deux courbes quelconques.* — Le théorème précédent s'applique de lui-même aux conjuguées de deux courbes

$$f(x,y)=0 \quad \text{et} \quad f_1(x,y)=0$$

qui passent en un point réel ou imaginaire commun aux deux lieux. C'est-à-dire que si deux équations

$$f(x,y)=0 \quad \text{et} \quad f_1(x,y)=0$$

ont une solution commune $[x, y]$ et qu'au point correspondant les $n$ premières dérivées de $y$ par rapport à $x$ aient mêmes valeurs de part et d'autre, les conjuguées des deux courbes, dont la caractéristique serait celle du point $[x, y]$, auront en ce point un contact de l'ordre $n$.

Car la condition que la caractéristique reste constante, fournira une équation $\beta' = \beta c$ parfaitement équivalente à une condition $\varphi(\alpha, \beta) = 0$.

**135.** Il résulte de ce qui précède que si l'on détermine, au moyen des formules usuelles, les coefficients A, B, R de l'équation

$$(x-A)^2 + (y-B)^2 = R^2,$$

de manière que cette équation admette une solution réelle ou imaginaire $[x, y]$, d'une équation $f(x,y)=0$, et fournisse de plus, au point correspondant, pour $\frac{dy}{dx}$ et $\frac{d^2y}{dx^2}$, les mêmes valeurs que donnerait l'équation $f(x,y)=0$ elle-même, les conjuguées des deux lieux auront au point $[x, y]$ même centre et même rayon de courbure.

La recherche du centre et du rayon de courbure d'une conjuguée d'une courbe quelconque en un point de cette conjuguée revient donc à la recherche du centre et du rayon de courbure de la conjuguée du *cercle imaginaire osculateur en ce point à la courbe proposée.*

De sorte que la question des courbures des courbes imaginaires est ramenée à celle des courbures des conjuguées du lieu

$$(x-A)^2 + (y-B)^2 = R^2.$$

Nous devons donc commencer par discuter ces conjuguées.

**156**. *Du cercle imaginaire.* — Les conjuguées que peut représenter l'équation

$$(x - a - a'\sqrt{-1})^2 + (y - b - b'\sqrt{-1})^2 = (r + r'\sqrt{-1})^2$$

ne changeant pas, quelque transformation qu'on fasse subir aux axes de coordonnées, nous les ferons tourner autour de l'origine d'un angle tel, que la partie imaginaire de l'ordonnée du centre disparaisse.

La transformation n'affectera jamais le rayon, qui restera toujours représenté par $r + r'\sqrt{-1}$; quant aux coordonnées du centre, la transformation les changera de la même manière que si elle ne se faisait que pour ce point. De sorte que si $\omega$ désigne l'angle dont on aura fait tourner les axes, l'équation nouvelle du lieu sera

$$\left[x - (a + a'\sqrt{-1})\cos\omega + (b + b'\sqrt{-1})\sin\omega\right]^2$$
$$+ \left[y - (a + a'\sqrt{-1})\sin\omega - (b + b'\sqrt{-1})\cos\omega\right]^2 = (r + r'\sqrt{-1})^2.$$

On fera donc disparaître la partie imaginaire de l'ordonnée du centre en faisant

$$\operatorname{tang}\omega = -\frac{b'}{a'}.$$

L'équation du lieu ainsi simplifiée sera

$$(x - a - a'\sqrt{-1})^2 + (y - b)^2 = (r + r'\sqrt{-1})^2;$$

en transportant ensuite les axes parallèlement à eux-mêmes au point réel $[a, b]$, on ramènera cette équation à la forme

$$(x - a\sqrt{-1})^2 + y^2 = (r + r'\sqrt{-1})^2.$$

C'est cette équation que nous allons discuter.

Nous déterminerons d'abord l'enveloppe imaginaire des courbes qu'elle représente.

Les coordonnées d'un point de l'enveloppe étant

$$x = \alpha + \beta\sqrt{-1}, \quad y = \alpha' + \beta'\sqrt{-1},$$

la condition que devront remplir les variables $\alpha$, $\beta$, $\alpha'$, $\beta'$ sera

$$\frac{dy}{dx} = -\frac{x - a\sqrt{-1}}{y} = -\frac{\alpha + (\beta - a)\sqrt{-1}}{\alpha' + \beta'\sqrt{-1}} = \text{réel},$$

c'est-à-dire

$$\frac{\alpha}{\alpha'} = \frac{\beta - a}{\beta'},$$

équation qu'il faudra adjoindre à celles qui exprimeraient que le point $[x, y]$ appartient au lieu proposé, et qui sont

$$\alpha^2 - (\beta - a)^2 + \alpha'^2 - \beta'^2 = r^2 - r'^2,$$

$$\alpha(\beta - a) + \alpha'\beta' = rr'.$$

En éliminant successivement $\beta$ et $\beta'$ d'abord, ensuite $\alpha$ et $\alpha'$ entre ces équations, on trouve

$$\alpha^2 + \alpha'^2 = r^2$$

et

$$(\beta - a)^2 + \beta'^2 = r'^2.$$

Il résulte de ces équations que l'enveloppe cherchée est la circonférence décrite du point $[x = a, y = 0]$ comme centre, avec un rayon égal à $r + r'$.

En effet, d'après l'équation

$$\alpha^2 + \alpha'^2 = r^2,$$

les coordonnées d'un point N quelconque (*fig.* 9) de la circonférence décrite autour de l'origine, avec un rayon $r$, sont des valeurs conjointes de $\alpha$ et de $\alpha'$; et de même, d'après l'équation

$$(\beta - a)^2 + \beta'^2 = r'^2,$$

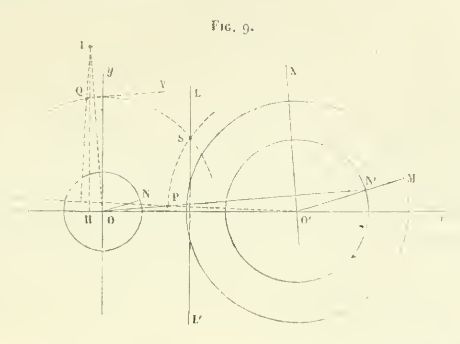
les coordonnées d'un point N' quelconque de la circonférence décrite autour du point O' $[x = a, y = 0]$ avec un rayon $r'$, sont aussi des valeurs conjointes de $\beta$ et de $\beta'$; mais d'un autre côté, en raison de

l'équation

$$\frac{\alpha}{\alpha'} = \frac{\beta - a}{\beta'},$$

les quatre valeurs conjointes de $\alpha$, $\alpha'$, $\beta$, $\beta'$ doivent être les coordonnées de points N et N' situés aux extrémités de rayons parallèles ON, O'N' des deux circonférences.

Fig. 9.




$\alpha + \beta$ et $\alpha' + \beta'$ sont donc les coordonnées du point M situé sur la circonférence décrite du point O' comme centre, avec un rayon égal à $r + r'$, à l'extrémité du rayon de cette circonférence qui se trouve couché sur O'N'.

Ainsi l'enveloppe imaginaire des conjuguées du lieu

$$(x - a\sqrt{-1})^2 + y^2 = (r + r'\sqrt{-1})^2$$

est le cercle

$$(x - a)^2 + y^2 = (r + r')^2.$$

Si l'on avait conservé à l'équation du cercle imaginaire sa forme primitive

$$(x - a - a'\sqrt{-1})^2 + (y - b - b'\sqrt{-1})^2 = (r + r'\sqrt{-1})^2,$$

on aurait trouvé pour équation en coordonnées réelles de l'enveloppe

imaginaire

$$(x-a-a')^2+(y-b-b')^2=(r+r')^2.$$

Ce résultat est remarquable.

Pour obtenir le point de contact M d'une conjuguée désignée C avec l'enveloppe, il suffira de construire le point N' qui lui correspond, car en prolongeant ensuite O'N' on aura le point M ; or les coordonnées $\beta'$ et $\beta$ du point N' devant fournir un rapport égal à C, on obtiendra ce point en menant la droite ON' dont l'angle avec l'axe des $x$ ait pour tangente C.

Lorsque l'origine sera dans l'intérieur du cercle O'N', le rapport des coordonnées du point N' pourra passer par tous les états de grandeur et, dans ce cas, toutes les conjuguées toucheront l'enveloppe chacune en deux points. Dans le cas contraire, les valeurs extrêmes du rapport des coordonnées du point N' seront les coefficients angulaires des tangentes menées de l'origine au cercle O'N' ; les conjuguées dont la caractéristique resterait comprise entre ces limites toucheront donc seules l'enveloppe imaginaire.

L'équation

$$\left(x-a\sqrt{-1}\right)^2+y^2=\left(r+r'\sqrt{-1}\right)^2$$

fournira dans ce dernier cas deux points réels par où passeront toutes les conjuguées. En effet les valeurs réelles de $x$ et de $y$ que pourrait comporter cette équation seraient

$$x=-\frac{rr'}{a} \quad \text{et} \quad y=\pm\frac{\sqrt{(a^2+r^2)(a^2-r'^2)}}{a},$$

mais la réalité des ordonnées dépend de la condition $a^2>r'^2$.

Si $a^2$ était égal à $r'^2$, c'est-à-dire si le cercle O'N' passait par l'origine, les deux points réels se confondraient en un seul et avec l'une des extrémités du diamètre horizontal du cercle ON.

Nous avons supposé, en faisant la figure, que $r$ et $r'$ fussent de même signe ; autrement les rayons ON et O'N' devraient être de sens contraires, et, par suite, le rayon O'M de l'enveloppe, toujours repré-

senté par $r+r'$, serait la différence des rayons ON et O′N′. En effet, les équations

$$\frac{\alpha}{\alpha'}=\frac{\beta-a}{\beta'}$$

et

$$\alpha(\beta-a)+\alpha'\beta'=rr',$$

qui se rapportent à un point quelconque de l'enveloppe, montrent, la première, que $\frac{\alpha}{\beta-a}$ et $\frac{\alpha'}{\beta'}$, ou, par suite, $\alpha(\beta-a)$ et $\alpha'\beta'$, sont toujours de même signe, tandis que la seconde exige ensuite que ces produits ou rapports aient le signe de $rr'$. De sorte que si $rr'$ est négatif, $\frac{\alpha}{\beta-a}$ et $\frac{\alpha'}{\beta'}$ étant négatifs, les rayons ON, O′N′ sont de sens contraires.

On peut construire par points, avec la règle et le compas, les conjuguées du cercle imaginaire

$$(x-a\sqrt{-1})^2+y^2=(r+r'\sqrt{-1})^2.$$

En effet,

$$x=\alpha+\beta\sqrt{-1}\quad \text{et}\quad y=\alpha'+\beta'\sqrt{-1}$$

désignant maintenant les coordonnées d'un point de la conjuguée C, on doit avoir

$$\alpha^2+\alpha'^2-r^2=(\beta-a)^2+\beta'^2-r'^2,$$

$$\alpha(\beta-a)+\alpha'\beta'=rr'$$

et

$$\frac{\beta'}{\beta}=\text{C}.$$

La première de ces équations exprime que les tangentes menées du point $[\alpha,\alpha']$ au cercle

$$y^2+x^2=r^2$$

sont égales aux tangentes menées du point $[\beta,\beta']$ au cercle

$$y^2+(x-a)^2=r'^2.$$

LL′ étant donc l'axe radical de ces deux cercles O et O′, si l'on marque un point S quelconque de cet axe et qu'on décrive les deux circonférences OS et O′S, $[\alpha, \alpha']$ seront les coordonnées d'un point de la première et $[\beta, \beta']$ celles d'un point de la seconde. Comme $\frac{\beta'}{\beta} = C$, le point $[\beta, \beta']$ se trouvera au point de rencontre de la circonférence O′S et de la droite fixe ON′ que l'on aura menée pour obtenir le point de contact M de la conjuguée C avec l'enveloppe. Ce point $[\beta, \beta']$ sera en P par exemple. D'un autre côté, $\alpha$ et $\alpha'$ doivent satisfaire à la condition

$$\alpha(\beta - a) + C\alpha'\beta = rr'$$

ou

$$\beta(\alpha + C\alpha') - a\alpha - rr' = 0.$$

Or cette équation, en y considérant $\alpha$ et $\alpha'$ comme les coordonnées courantes, représente une droite qui, quel que soit $\beta$, passe toujours au point fixe

$$\alpha = -\frac{rr'}{a}, \quad \alpha' = \frac{rr'}{aC}$$

et dont le coefficient angulaire

$$-\frac{\beta - a}{C\beta} \quad \text{ou} \quad -\frac{\beta - a}{\beta'}$$

est l'inverse changée de signe du coefficient angulaire de O′P. Ces deux conditions la déterminent, et il en résulte que le point $[\beta, \beta']$ de la circonférence OS, qui correspond au point $[\alpha, \alpha']$ de la circonférence O′S, doit être sur la perpendiculaire menée à O′P du point fixe

$$\left[-\frac{rr'}{a}, \frac{rr'}{aC}\right].$$

Ce dernier point est en I, à la rencontre de la ligne HI,

$$x = -\frac{rr'}{a},$$

qui passe par les deux points réels, et de la perpendiculaire OI à ON′.

Par conséquent si IQ est perpendiculaire à O′ P, Q est l'un des points cherchés.

Les points P et Q étant ainsi déterminés, le point correspondant V du lieu s'obtiendra en menant de Q une droite QV égale et parallèle à OP.

Les asymptotes de toutes les conjuguées sont représentées par les équations

$$y = \pm \sqrt{-1}\,(x - a\sqrt{-1});$$

celles de la conjuguée C sont donc, en coordonnées réelles.

$$y = \frac{C-1}{C+1}\,x + a$$

et

$$y = \frac{1+C}{1-C}\,x - a.$$

Les deux asymptotes d'une même conjuguée sont en conséquence toujours perpendiculaires l'une sur l'autre; elles partent respectivement des points $[0, +a]$, $[0, -a]$ et enfin sont inclinées de 45° sur la droite $y = Cx$. Quant à leur point de rencontre, il décrit la circonférence du cercle $y^2 + x^2 = a^2$ et de plus appartient à la perpendiculaire O′X menée à la droite ON′, $y = Cx$, car les équations de ces asymptotes donnent

$$(C+1)\,y = (C-1)\,x + a\,(C+1)$$

et

$$(1-C)\,y = (1+C)\,x - a\,(1-C).$$

d'où l'on tire par soustraction

$$y = -\frac{1}{C}\,(x - a).$$

Au reste la ligne O′X,

$$y = -\frac{1}{C}\,(x - a),$$

est un axe de symétrie de la conjuguée C. La règle qui a été donnée

pour la construction des points de cette conjuguée le montre suffisamment.

*Remarque.* — Les conjuguées du cercle imaginaire, dont la construction par points est, comme on vient de le voir, toujours si facile, sont remarquables à plus d'un titre. En les projetant d'un plan sur un autre, on en tirerait d'abord toutes les courbes que peut représenter l'équation

$$\begin{gathered} Ay^2 + Bxy + Cx^2 \\ + (D + D'\sqrt{-1})\,y + (E + E'\sqrt{-1})\,x + F + F'\sqrt{-1} = 0; \end{gathered}$$

mais celles-ci fourniront ensuite, comme on le verra plus tard, toutes les courbes du quatrième ordre dont l'équation peut être abaissée au second degré en substituant la représentation en coordonnées imaginaires à la représentation en coordonnées réelles.

Or ces courbes jouissent de propriétés toutes caractéristiques : elles n'ont que deux tangentes parallèles à une direction donnée, elles n'ont que deux asymptotes, elles ont toujours un diamètre rectiligne; enfin leurs aires peuvent s'exprimer au moyen seulement des fonctions circulaires et sont, par suite, simplement périodiques.

Ces courbes formeraient donc, parmi celles du quatrième ordre, une classe fort intéressante, à ces divers titres, mais de plus assez étendue, puisque leur équation contiendrait dix constantes arbitraires sur quatorze qui peuvent entrer dans l'équation générale du quatrième degré.

**157.** La détermination des courbures des lieux plans réels ou imaginaires se trouve, par ce qui précède, ramenée à la détermination des courbures des conjuguées du cercle imaginaire

$$(x - a - a'\sqrt{-1})^2 + (y - b - b'\sqrt{-1})^2 = (r + r'\sqrt{-1}).$$

Deux méthodes bien différentes se présentent d'elles-mêmes pour cette dernière recherche, comme au reste pour toutes celles qui nous ont déjà occupé.

Si l'on ne peut mieux faire, on repassera, des équations entre les

formes imaginaires des variables considérées, aux équations entre les valeurs réelles de ces variables, pour n'avoir plus qu'à appliquer les formules usuelles de solution des questions qu'on se proposait.

Mais si l'on a pu au contraire concevoir d'abord à la question posée une réponse intelligible, quoique compliquée par la présence d'imaginaires, on conservera aux données leur forme primitive imaginaire, pour en former directement le résultat cherché, sous sa forme imaginaire prévue et interprétée d'avance.

La première méthode, en raison même des moyens dont elle dispose, ne peut conduire qu'à des résultats informes; elle ne constitue donc qu'une ressource insuffisante pour les cas où l'on n'aurait pu instituer la seconde : aussi est-ce à permettre d'en éviter l'emploi que tend la théorie tout entière, puisque ce ne serait rien en effet que d'avoir su attribuer la forme imaginaire aux données réelles d'une question, s'il fallait, pour traiter cette question, rendre avant tout aux données leur forme réelle.

La solution que nous allons proposer de la question qui nous occupe se trouverait donc condamnée à l'avance par les raisons que nous venons d'indiquer. On ne doit en effet la considérer que comme provisoire.

Au reste, nous bornons ici nos recherches à la détermination du rayon de courbure de l'enveloppe imaginaire des conjugués d'une courbe quelconque et à celle du rayon de courbure d'une conjuguée aux points seulement où elle touche l'une ou l'autre enveloppe.

Les résultats auxquels nous sommes parvenu étant assez simples pour pouvoir être conservés sous leur forme actuelle, quelques progrès qu'on puisse faire plus tard dans la solution générale de la question, nous pouvons donc les noter.

**158.** *De la courbure de l'enveloppe imaginaire des lieux plans représentés par une équation entre deux variables.* — Lorsque deux équations admettent une solution commune et qu'au point correspondant les valeurs de $\frac{dy}{dx}$ sont, de part et d'autre, réelles et égales, les deux enveloppes passent en ce point et s'y touchent : il était donc présumable que si les valeurs de $\frac{d^2y}{dx^2}$ se trouvaient encore les mêmes

de part et d'autre, au point considéré, les deux enveloppes y auraient un contact du second ordre et par conséquent même centre et même rayon de courbure.

La démonstration positive du fait présentait toutefois des difficultés inattendues. Les deux enveloppes, une fois tracées, remplissent bien en effet la condition graphique énoncée, mais sans cependant que les conditions supposées entraînent l'existence simultanée sur les deux enveloppes de trois points ayant identiquement les mêmes coordonnées. Les grandeurs des coordonnées du troisième point réalisées sont bien les mêmes de part et d'autre, mais les valeurs algébriques imaginaires de ces coordonnées ne sont point pareilles. La répartition en parties réelles et imaginaires des coordonnées réalisées de ce troisième point peut différer d'une enveloppe à l'autre, les sommes seules des parties réelles et imaginaires des deux coordonnées restent identiques.

Lorsque ce théorème sera établi, on pourra prendre pour centre et pour rayon de courbure de l'enveloppe imaginaire des conjuguées d'un lieu quelconque, en un point de cette enveloppe, le centre et le rayon de courbure de l'enveloppe imaginaire des conjuguées du cercle osculateur, en ce point, au lieu considéré.

Soit donc $[x, y]$ le point commun aux enveloppes imaginaires des conjuguées de deux lieux et supposons que $\frac{dy}{dx}$ et $\frac{d^2y}{dx^2}$ aient de part et d'autre les mêmes valeurs en ce point, $\frac{dy}{dx}$ y étant d'ailleurs réel.

Si $p$ désigne la valeur réelle de $\frac{dy}{dx}$ au point $[x, y]$,

$$dy = d\alpha' + d\beta'\sqrt{-1}$$

et

$$dx = d\alpha + d\beta\sqrt{-1},$$

devront satisfaire à la condition

$$\frac{d\alpha' + d\beta'\sqrt{-1}}{d\alpha + d\beta\sqrt{-1}} = p,$$

qui donne

$$\frac{d\alpha'}{d\alpha} = p \quad \text{et} \quad \frac{d\beta'}{d\beta} = \frac{\frac{d\beta'}{d\alpha}}{\frac{d\beta}{d\alpha}} = p;$$

d'un autre côté, si $r + s\sqrt{-1}$ est la valeur de $\frac{d^2y}{dx^2}$ au point $[x, y]$, la valeur de $\frac{dy}{dx}$ en un point du lieu, voisin de $[x, y]$, sera représentée par

$$\frac{dY}{dX} = p + (r + s\sqrt{-1})\frac{X - x}{1} + \ldots,$$

et pour que le point

$$\left[x + d\alpha + d\beta\sqrt{-1},\ y + d\alpha' + d\beta'\sqrt{-1}\right]$$

appartienne aussi à l'enveloppe, il faudra que l'accroissement

$$(r + s\sqrt{-1})(d\alpha + d\beta\sqrt{-1}),$$

qu'aura subi la dérivée de Y par rapport à X, en passant du premier point au second, soit réel. Cette condition donne

$$s\,d\alpha + r\,d\beta = 0$$

ou

$$\frac{d\beta}{d\alpha} = -\frac{s}{r}.$$

Ainsi au point commun aux deux enveloppes considérées, puisque $p$, $r$ et $s$ sont supposés les mêmes de part et d'autre, $\frac{d\beta}{d\alpha}$, $\frac{d\alpha'}{d\alpha}$ et $\frac{d\beta'}{d\alpha}$ auront les mêmes valeurs de part et d'autre.

Passons aux dérivées secondes $\frac{d^2\beta}{d\alpha^2}$, $\frac{d^2\alpha'}{d\alpha^2}$ et $\frac{d^2\beta'}{d\alpha^2}$ : de quelque point $[x, y]$ qu'il s'agisse, on a toujours identiquement

$$\frac{dY}{dX} = \frac{dY}{d\alpha}\frac{d\alpha}{dX} = \left(\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}\sqrt{-1}\right)\frac{1}{1 + \frac{d\beta}{d\alpha}\sqrt{-1}}.$$

et, par suite,

$$\frac{d^2 Y}{dX^2} = \frac{d\left(\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}\sqrt{-1}\right)}{d\alpha} \frac{1}{\left(1 + \frac{d\beta}{d\alpha}\sqrt{-1}\right)^2} - \left(\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}\sqrt{-1}\right) \frac{\frac{d^2\beta}{d\alpha^2}\sqrt{-1}}{\left(1 + \frac{d\beta}{d\alpha}\sqrt{-1}\right)^3}$$

$$= \frac{\left(\frac{d^2\alpha'}{d\alpha^2} + \frac{d^2\beta'}{d\alpha^2}\sqrt{-1}\right)\left(1 + \frac{d\beta}{d\alpha}\sqrt{-1}\right) - \left(\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}\sqrt{-1}\right)\frac{d^2\beta}{d\alpha^2}\sqrt{-1}}{\left(1 + \frac{d\beta}{d\alpha}\sqrt{-1}\right)^3}.$$

Les dérivées secondes de Y par rapport à X au point $[x, y]$ étant donc supposées égales de part et d'autre et leur valeur commune étant $r + s\sqrt{-1}$, on aura pour l'un et l'autre lieu

$$r + s\sqrt{-1} = \frac{\left(\frac{d^2\alpha'}{d\alpha^2} + \frac{d^2\beta'}{d\alpha^2}\sqrt{-1}\right)\left(1 + \frac{d\beta}{d\alpha}\sqrt{-1}\right) - \left(\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}\sqrt{-1}\right)\frac{d^2\beta}{d\alpha^2}\sqrt{-1}}{\left(1 + \frac{d\beta}{d\alpha}\sqrt{-1}\right)^3}.$$

En remplaçant dans cette équation $\frac{d\beta}{d\alpha}$ par $-\frac{s}{r}$, $\frac{d\alpha'}{d\alpha}$ par $p$, et $\frac{d\beta'}{d\alpha}$ par $-\frac{ps}{r}$, valeurs trouvées plus haut, et décomposant, on trouve

$$r^3 \frac{d^2\alpha'}{d\alpha^2} + r^2 s\left(\frac{d^2\beta'}{d\alpha^2} - p\frac{d^2\beta}{d\alpha^2}\right) = r^4 - s^4$$

et

$$rs\frac{d^2\alpha'}{d\alpha^2} - r^2\left(\frac{d^2\beta'}{d\alpha^2} - p\frac{d^2\beta}{d\alpha^2}\right) = 2s(r^2 + s^2),$$

d'où l'on conclut

$$\frac{d^2\alpha'}{d\alpha^2} = \frac{r^2 + s^2}{r}$$

et

$$\frac{d^2\beta'}{d\alpha^2} - p\frac{d^2\beta}{d\alpha^2} = -\frac{s}{r}\frac{d^2\alpha'}{d\alpha^2} = -\frac{s}{r^2}(r^2 + s^2)\ [*].$$

---

[*] L'équation

$$\frac{d^2\beta'}{d\alpha^2} - p\frac{d^2\beta}{d\alpha^2} = -\frac{s}{r}\frac{d^2\alpha'}{d\alpha^2}$$

Ces deux dernières équations ne se rapportent pas plus à l'enveloppe imaginaire des conjuguées qu'à tout autre lieu partant du point

$$[x + d\alpha + d\beta\sqrt{-1},\ y + d\alpha' + d\beta'\sqrt{-1}]$$

de l'enveloppe. Aussi contiennent-elles trois inconnues $\frac{d^2\alpha'}{d\alpha^2}$, $\frac{d^2\beta}{d\alpha^2}$ et $\frac{d^2\beta'}{d\alpha^2}$ et, par suite, laissent-elles l'une d'elles indéterminée.

Mais ce que la question offre de particulier, c'est que les données ne suffisent pas pour achever la détermination de $\frac{d^2\beta}{d\alpha^2}$ et de $\frac{d^2\beta'}{d\alpha^2}$ qui restent liées entre elles par la seule condition

$$\frac{d^2\beta'}{d\alpha^2} - p\frac{d^2\beta}{d\alpha^2} = -\frac{s}{r^2}(r^2 + s^2).$$

Il est évident en effet que, pour exprimer que le troisième point est aussi resté sur l'enveloppe, il faudrait exprimer que le nouvel accroissement subi par $\frac{dY}{dX}$ est encore resté réel ; or l'expression de cette condition renfermerait les parties réelle et imaginaire de $\frac{d^3Y}{dX^3}$ au point $[x, y]$, parties que l'on ne connaît pas.

Les valeurs de $\frac{d^3Y}{dX^3}$ n'étant donc pas supposées les mêmes pour les deux lieux, au point $[x, y]$, $\frac{d^2\alpha'}{d\alpha^2}$ aura bien de part et d'autre la même valeur, puisque les conditions précédentes l'ont séparé; mais $\frac{d^2\beta}{d\alpha^2}$ et

---

se retrouverait en dérivant par rapport à $\alpha$ l'équation

$$\frac{d\alpha'}{d\alpha} = \frac{\frac{d\beta'}{d\alpha}}{\frac{d\beta}{d\alpha}},$$

qui exprime que $\frac{dy}{dx}$ est resté réel en passant du point $[x, y]$ au point

$$[x + d\alpha + d\beta\sqrt{-1},\ y + d\alpha' + d\beta'\sqrt{-1}].$$

$\frac{d^2\beta'}{d\alpha^2}$ pourront être différents et seront seulement liés l'un à l'autre par la même condition

$$\frac{d^2\beta'}{d\alpha^2} - p\frac{d^2\beta}{d\alpha^2} = -\frac{s}{r^2}(r^2 + s^2).$$

Les deux enveloppes auront cependant au point $[x, y]$ la même courbure et le même centre de courbure, puisqu'elles passent toutes deux au point $[x, y]$, qu'elles y ont la même tangente sous le coefficient angulaire $p$; qu'elles contiennent par conséquent toutes deux le point

$$[x + d\alpha + d\beta\sqrt{-1},\ y + d\alpha' + d\beta'\sqrt{-1}],$$

défini par les conditions

$$\frac{d\alpha'}{d\alpha} = p,\quad \frac{d\beta}{d\alpha} = -\frac{s}{r},\quad \frac{d\beta'}{d\alpha} = -p\frac{s}{r},$$

et qu'enfin elles ont encore en ce point

$$[x + d\alpha + d\beta\sqrt{-1},\ y + d\alpha' + d\beta'\sqrt{-1}]$$

meme tangente, sous le coefficient angulaire

$$p + r\,d\alpha - s\,d\beta.$$

Pour concilier ces résultats, en apparence contradictoires, il faut donc que la courbure de l'une et de l'autre enveloppe ne dépende pas séparément de $\frac{d^2\beta}{d\alpha^2}$ et de $\frac{d^2\beta'}{d\alpha^2}$ au point commun, mais seulement de la somme

$$\frac{d^2\beta'}{d\alpha^2} - p\frac{d^2\beta}{d\alpha^2}.$$

La vérification de ce point est en effet aisée à produire.

Car si $x_1$ et $y_1$ désignent les coordonnées réalisées d'un point quelconque d'un lieu imaginaire, la courbure de ce lieu au point $[x_1, y_1]$

dépend de $\frac{dy_1}{dx_1}$ et de $\frac{d^2y_1}{dx_1^2}$; or

$$\frac{dy_1}{dx_1} = \frac{d\alpha' + d\beta'}{d\alpha + d\beta} = \frac{\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}}{1 + \frac{d\beta}{d\alpha}}$$

et

$$\frac{d^2y_1}{dx_1^2} = \frac{d\,\frac{\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}}{1 + \frac{d\beta}{d\alpha}}}{d\alpha}\,\frac{d\alpha}{dx_1} = \frac{d\,\frac{\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}}{1 + \frac{d\beta}{d\alpha}}}{d\alpha}\cdot\frac{1}{1 + \frac{d\beta}{d\alpha}}$$

$$= \frac{\left(\frac{d^2\alpha'}{d\alpha^2} + \frac{d^2\beta'}{d\alpha^2}\right)\left(1 + \frac{d\beta}{d\alpha}\right) - \left(\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}\right)\frac{d^2\beta}{d\alpha^2}}{\left(1 + \frac{d\beta}{d\alpha}\right)^3}.$$

Mais au point commun aux deux enveloppes qui nous occupent, $\frac{d\beta}{d\alpha}$, $\frac{d\alpha'}{d\alpha}$ et $\frac{d\beta'}{d\alpha}$ ont identiquement les mêmes valeurs, $\frac{dy_1}{dx_1}$ a donc de part et d'autre la même valeur; d'un autre côté, si l'on remplace, dans l'expression de $\frac{d^2y_1}{dx_1^2}$, $\frac{d\beta}{d\alpha}$, $\frac{d\alpha'}{d\alpha}$ et $\frac{d\beta'}{d\alpha}$ par leurs valeurs trouvées plus haut,

$$\frac{d\beta}{d\alpha} = -\frac{s}{r}, \quad \frac{d\alpha'}{d\alpha} = p, \quad \frac{d\beta'}{d\alpha} = -\frac{ps}{r},$$

il vient

$$\frac{d^2y_1}{dx_1^2} = \frac{\left(\frac{d^2\alpha'}{d\alpha^2} + \frac{d^2\beta'}{d\alpha^2}\right)\left(1 - \frac{s}{r}\right) - \left(p - \frac{ps}{r}\right)\frac{d^2\beta}{d\alpha^2}}{\left(1 - \frac{s}{r}\right)^3}:$$

cette expression ne dépend en effet que de la somme

$$\frac{d^2\beta'}{d\alpha^2} - p\,\frac{d^2\beta}{d\alpha^2}.$$

Ainsi quand on applique à un point $[x, y]$ de l'enveloppe imagi-

naire des conjuguées d'un lieu $f(x, y) = 0$, les formules qui fourniraient le centre et le rayon de courbure de la courbe en un de ses points réels, l'enveloppe imaginaire des conjuguées du lieu représenté par l'équation du cercle osculateur, alors imaginaire, que donnent les formules, passe au point $[x, y]$, et les deux enveloppes y ont même centre et même rayon de courbure.

Mais si l'équation du cercle osculateur est

$$(x - a - a'\sqrt{-1})^2 + (y - b - b'\sqrt{-1})^2 = (r + r'\sqrt{-1})^2,$$

l'enveloppe imaginaire des conjuguées coïncide avec le cercle réel

$$(x - a - a')^2 + (y - b - b')^2 = (r + r')^2,$$

c'est-à-dire que le centre de courbure de cette enveloppe est le point $[a + a', b + b']$ et sa courbure $\frac{1}{r + r'}$.

Par conséquent donc, si en un point quelconque $[x, y]$ de l'enveloppe imaginaire des conjuguées d'un lieu $f(x, y) = 0$ on a calculé les valeurs $a + a'\sqrt{-1}$, $b + b'\sqrt{-1}$ et $(r + r'\sqrt{-1})^2$ de

$$x + \frac{\left[1 + \left(\frac{dy}{dx}\right)^2\right]\frac{dy}{dx}}{\frac{d^2y}{dx^2}},$$

$$y + \frac{1 + \left(\frac{dy}{dx}\right)^2}{\frac{d^2y}{dx^2}}$$

et

$$\frac{\left[1 + \left(\frac{dy}{dx}\right)^2\right]^3}{\left(\frac{d^2y}{dx^2}\right)^2},$$

le cercle osculateur de cette enveloppe au point considéré sera

$$(x - a - a')^2 + (y - b - b')^2 = (r + r')^2.$$

Ce théorème aidera beaucoup à la construction toujours si importante de l'enveloppe imaginaire des conjuguées du lieu dont on s'occupera.

**139.** *De la courbure d'une conjuguée quelconque en un point où elle touche l'une ou l'autre enveloppe.* — On pourrait établir très-simplement que les courbures de la courbe réelle et d'une quelconque de ses conjuguées, aux points où elles se touchent, sont toujours égales et opposées : en effet, quelle qu'en soit la cause, le fait est vrai pour le cercle et ses conjuguées hyperboliques ; or il en résulte que si l'on a déterminé le cercle osculateur à une courbe réelle en un de ses points réels, la conjuguée de ce cercle, qui passera au même point, aura sa courbure réelle et opposée à celle de la courbe réelle; et comme d'un autre côté il a été établi que cette conjuguée du cercle aura, avec la conjuguée de la courbe réelle, qui la touche au même point, un contact du second ordre. La courbe réelle et sa conjuguée auront donc elles-mêmes, au point où elles se touchent, leurs courbures égales et opposées.

Quant à l'explication du fait, on la trouverait aisément dans la comparaison des termes de moindres degrés par rapport à $x$ et à $y$ des équations en coordonnées réelles de la courbe réelle et de sa conjuguée, rapportées toutes deux à leur tangente et à leur normale communes.

Mais nous n'insisterons pas, parce que la courbe réelle n'étant en définitive qu'une branche particulière de l'enveloppe totale, ses propriétés se déduisent, comme cas particuliers, de celles de l'enveloppe imaginaire.

**140.** Nous savons déjà que si l'on a déterminé le cercle imaginaire osculateur à une courbe $f(x, y) = 0$ en un point $[x, y]$ pris sur l'enveloppe imaginaire des conjuguées de cette courbe, non-seulement les deux enveloppes seront osculatrices l'une à l'autre, en ce point, mais encore les conjuguées qui y passeront le seront aussi.

En sorte que la recherche de la courbure d'une conjuguée en un point où elle touche l'enveloppe imaginaire revient à celle de la courbure en ce point de la conjuguée du cercle osculateur qui y passe.

Tout se réduit donc à obtenir le rayon et le centre de courbure d'une des conjuguées du lieu

$$(x - a - a'\sqrt{-1})^2 + (y - b - b'\sqrt{-1})^2 = (r + r'\sqrt{-1})^2,$$

au point où elle touche l'enveloppe imaginaire de ce lieu.

Soient en conséquence $x$ et $y$ les coordonnées d'un point de l'enveloppe des conjuguées du cercle imaginaire

$$(x - a - a'\sqrt{-1})^2 + (y - b - b'\sqrt{-1})^2 = (r + r'\sqrt{-1})^2.$$

Si l'on pose

$$x = \alpha + \beta\sqrt{-1} \quad \text{et} \quad y = \alpha' + \beta'\sqrt{-1},$$

il en résultera

(1) $$(\alpha - a)^2 - (\beta - a')^2 + (\alpha' - b)^2 - (\beta' - b')^2 = r^2 - r'^2$$

et

(2) $$(\alpha - a)(\beta - a') + (\alpha' - b)(\beta' - b') = rr',$$

et, pour exprimer que le point $[x, y]$ appartient à l'enveloppe, c'est-à-dire que $\frac{dy}{dx}$ est réel en ce point,

(3) $$\frac{\alpha - a}{\alpha' - b} = \frac{\beta - a'}{\beta' - b'}.$$

Mais ces trois équations n'entreront pas dans le calcul aux mêmes titres : les deux premières expriment simplement que le point

$$x = \alpha + \beta\sqrt{-1},$$
$$y = \alpha' + \beta'\sqrt{-1},$$

appartient au lieu considéré; on pourra donc les différentier une et deux fois pour passer du point $[x, y]$ aux points voisins de la conjuguée qui passe en ce point; tandis que l'équation (3) exprimant en

outre que le point $[x, y]$ appartient à l'enveloppe, ne convient qu'au point de départ.

Ainsi en désignant par $x_1$, $y_1$ les coordonnées réalisées d'un point quelconque de la conjuguée qui touche l'enveloppe imaginaire au point $[x, y]$, on pourra poser

$$x_1 = \alpha + \beta,$$
$$y_1 = \alpha' + \beta',$$

et les dérivées de $y_1$ par rapport à $x_1$ résulteront indirectement des équations dérivées des équations (1) et (2) et d'une condition particulière qui exprimera que le point $[x_1, y_1]$ se déplace sur la même conjuguée.

On aura en effet pour déterminer $\frac{dy_1}{dx_1}$ et $\frac{d^2y_1}{dx_1^2}$ les formules

$$\frac{dy_1}{dx_1} = \frac{d\alpha' + d\beta'}{d\alpha + d\beta} = \frac{\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}}{1 + \frac{d\beta}{d\alpha}}$$

et

$$\frac{d^2y_1}{dx_1^2} = \frac{d\cdot\frac{\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}}{1 + \frac{d\beta}{d\alpha}}}{d\alpha}\cdot\frac{d\alpha}{dx_1} = \frac{d\cdot\frac{\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}}{1 + \frac{d\beta}{d\alpha}}}{d\alpha}\cdot\frac{1}{1 + \frac{d\beta}{d\alpha}}$$

$$= \frac{\left(\frac{d^2\alpha'}{d\alpha^2} + \frac{d^2\beta'}{d\alpha^2}\right)\left(1 + \frac{d\beta}{d\alpha}\right) - \left(\frac{d\alpha'}{d\alpha} + \frac{d\beta'}{d\alpha}\right)\frac{d^2\beta}{d\alpha^2}}{\left(1 + \frac{d\beta}{d\alpha}\right)^3}.$$

Ainsi il ne reste qu'à tirer, en fonction de $\alpha$, $\beta$, $\alpha'$ et $\beta'$, les valeurs de $\frac{d\alpha'}{d\alpha}$, $\frac{d\beta}{d\alpha}$, $\frac{d\beta'}{d\alpha}$, $\frac{d^2\alpha'}{d\alpha^2}$, $\frac{d^2\beta}{d\alpha^2}$, et $\frac{d^2\beta'}{d\alpha^2}$, au moyen d'abord des équations différentielles des équations (1) et (2) et de la condition complémentaire $\frac{\beta'}{\beta}$ égale constante.

**141.** Mais on peut simplifier le calcul en se servant d'une remarque bonne à consigner, du reste, parce qu'elle pourra être souvent utile.

Voici le fait : lorsqu'on s'éloigne, sur une conjuguée quelconque, du point où elle touche l'une des deux enveloppes, les parties imaginaires des coordonnées varient seules, lorsque ce point appartient à l'enveloppe réelle, tandis que, dans le cas contraire, ce sont les parties réelles qui varient; c'est-à-dire que dans le premier cas $\frac{d\alpha}{d\beta}$ et $\frac{d\alpha'}{d\beta}$ ont pour limites o, tandis que $\frac{d\beta'}{d\beta}$ a pour valeur la caractéristique de la conjuguée, ou le coefficient angulaire de la tangente à l'enveloppe réelle au point considéré; et que dans le second cas, $\frac{d\beta}{d\alpha}$ et $\frac{d\beta'}{d\alpha}$ ont pour limites o, tandis que $\frac{d\alpha'}{d\alpha}$ a pour valeur le coefficient angulaire de la tangente à l'enveloppe imaginaire au point considéré.

En effet, dans le premier cas, où le point considéré appartient à l'enveloppe réelle, si l'on regarde la caractéristique C comme une fonction de $\alpha$ et de $\beta$, on pourra poser

$$dC = \frac{dC}{d\alpha}d\alpha + \frac{dC}{d\beta}d\beta.$$

Or la dérivée partielle $\frac{dC}{d\beta}$, prise en un point de l'enveloppe réelle, est toujours identiquement nulle; car si $\beta$ varie seul, pour que $\frac{dy}{dx}$, qui peut alors se mettre sous la forme $\frac{d\alpha' + d\beta'\sqrt{-1}}{d\beta\sqrt{-1}}$, ait la valeur C, il faut que $d\alpha' = 0$, et que $d\beta' = C d\beta$; de sorte que

$$C + dC = \frac{d\beta'}{d\beta} = C$$

et que par suite la dérivée partielle $\frac{dC}{d\beta}$ est identiquement nulle; d'un autre côté, la dérivée partielle $\frac{dC}{d\alpha}$ ne se trouve nulle qu'en des points

singuliers du lieu, sa valeur est habituellement donnée par celle de $\frac{d^2y}{dx^2}$ prise au point considéré de la courbe réelle.

Dans le cas donc où nous raisonnons,

$$dC = \frac{d^2y}{dx^2}\,d\alpha:$$

pour que $dC$ soit nul, c'est-à-dire pour que le point $[x, y]$ soit resté sur la même conjuguée, il faut donc que $d\alpha$ soit nul, et alors $d\alpha'$, comme on l'a déjà dit, est nul aussi.

Dans le second cas, où le point considéré appartient à l'enveloppe imaginaire, il suffit d'observer que si

$$dx = d\alpha + d\beta\sqrt{-1}$$

et que $p$ désigne la valeur réelle de $\frac{dy}{dx}$ au point considéré, la valeur de $dy$ sera

$$dy = pd\alpha + pd\beta\sqrt{-1},$$

de sorte que $\frac{d\beta'}{d\beta}$ ayant d'une part la valeur $p$, et devant de l'autre être égal à C, la conciliation n'est possible qu'en faisant $d\beta$ et $d\beta'$ nuls, c'est-à-dire

$$\frac{d\beta'}{d\beta} = \frac{\frac{d\beta'}{d\alpha}}{\frac{d\beta}{d\alpha}} = \frac{0}{0},$$

à moins que $p$ ne soit égal à C, ce qui n'arrive qu'en des points particuliers de l'enveloppe imaginaire.

**142.** Dans le cas qui nous occupe, du cercle imaginaire, $p$ est toujours différent de C; car la valeur de $p$, au point M de l'enveloppe (*fig.* 9), est le coefficient angulaire réel de la tangente à cette enveloppe, en ce point, tandis que la caractéristique du point M est le coefficient angulaire de ON'. Ainsi dans le calcul que nous nous proposons de faire, $\frac{d\beta}{d\alpha}$ et $\frac{d\beta'}{d\alpha}$ devront être faits nuls.

Cela posé, nous pourrons, pour simplifier les calculs, réduire notre recherche à ce qui concerne la conjuguée $C = 0$; cette hypothèse ne constitue pas un cas particulier, puisque les axes sont quelconques.

Dans ce cas, $\beta'$ restant constamment nul, $\frac{d^2\beta'}{d\alpha^2}$ sera nul aussi et les valeurs de $\frac{dy_1}{dx_1}$ et de $\frac{d^2y_1}{dx_1^2}$ se réduiront à

$$\frac{dy_1}{dx_1} = \frac{d\alpha'}{d\alpha},$$

$$\frac{d^2y_1}{dx_1^2} = \frac{d^2\alpha'}{d\alpha^2} - \frac{d\alpha'}{d\alpha}\frac{d^2\beta}{d\alpha^2}.$$

Les équations (1) et (2) différentiées une fois, par rapport à $\alpha$, en tenant compte des conditions

$$\beta' = 0, \quad \frac{d\beta}{d\alpha} = 0, \quad \frac{d\beta'}{d\alpha} = 0,$$

donnent

$$\alpha - a + (\alpha' - b)\frac{d\alpha'}{d\alpha} = 0$$

et

$$(\beta - a') - b'\frac{d\alpha'}{da} = 0;$$

mais ces deux relations se réduisent à une seule

$$\frac{d\alpha'}{da} = -\frac{\alpha - a}{\alpha' - b},$$

en vertu de la condition (3)

$$\frac{\alpha - a}{\alpha' - b} = \frac{\beta - a'}{\beta' - b'},$$

qui se réduit ici à

$$-\frac{\alpha - a}{\alpha' - b} = \frac{\beta - a'}{b'}.$$

Les mêmes équations (1) et (2) différentiées deux fois, par rapport

à $\alpha$, en tenant compte des conditions

$$\beta' = 0, \quad \frac{d\beta}{d\alpha} = 0, \quad \frac{d\beta'}{d\alpha} = 0, \quad \frac{d^2\beta'}{d\alpha^2} = 0,$$

donnent

$$1 + \left(\frac{d\alpha'}{d\alpha}\right)^2 + (\alpha' - b)\frac{d^2\alpha'}{d\alpha^2} - (\beta - a')\frac{d^2\beta}{d\alpha^2} = 0$$

et

$$- b'\frac{d^2\alpha'}{d\alpha^2} + (\alpha - a)\frac{d^2\beta}{d\alpha^2} = 0;$$

on en tire

$$\frac{d^2\alpha'}{d\alpha^2} = - \frac{(\alpha - a)\left[1 + \left(\frac{d\alpha'}{d\alpha}\right)^2\right]}{(\alpha' - b)(\alpha - a) - b'(\beta - a')}$$

et

$$\frac{d^2\beta}{d\alpha^2} = \frac{- b'\left[1 + \left(\frac{d\alpha'}{d\alpha}\right)^2\right]}{(\alpha' - b)(\alpha - a) - b'(\beta - a')},$$

ou bien

$$\frac{d^2\alpha'}{d\alpha^2} = \frac{-(\alpha - a)[(\alpha - a)^2 + (\alpha' - b)^2]}{(\alpha' - b)^2[(\alpha' - b)(\alpha - a) - b'(\beta - a')]}$$

et

$$\frac{d^2\beta}{d\alpha^2} = \frac{- b'[(\alpha - a)^2 + (\alpha' - b)^2]}{(\alpha' - b)^2[(\alpha' - b)(\alpha - a) - b'(\beta - a')]};$$

ou, en remplaçant $\beta - a'$ par sa valeur tirée de l'équation (3) réduite à $\frac{\alpha - a}{\alpha' - b} = - \frac{\beta - a'}{b'}$,

$$\frac{d^2\alpha'}{d\alpha^2} = \frac{-[(\alpha - a)^2 + (\alpha' - b)^2]}{(\alpha' - b)[(\alpha' - b)^2 + b'^2]}$$

et

$$\frac{d^2\beta}{d\alpha^2} = \frac{- b'[(\alpha - a)^2 + (\alpha' - b)^2]}{(\alpha' - b)(\alpha - a)[(\alpha' - b)^2 + b'^2]}.$$

Il en résulte d'abord

$$\frac{d^2\beta}{d\alpha^2}\frac{d\alpha'}{d\alpha} = \frac{b'[(\alpha - a)^2 + (\alpha' - b)^2]}{(\alpha' - b)^2[(\alpha' - b)^2 + b')]},$$

et, par suite,

$$\frac{dy_1}{dx_1} = -\frac{\alpha - a}{\alpha' - b}$$

et

$$\frac{d^2y_1}{dx_1^2} = -\frac{(\alpha - a)^2 + (\alpha' - b)^2}{(\alpha' - b)^2[(\alpha' - b)^2 + b'^2]}[(\alpha' - b) + b'].$$

Cela posé, il ne reste plus qu'à obtenir $\alpha - a$ et $\alpha' - b$, on les tirerait des équations (1), (2) et (3) après y avoir fait $\beta' = 0$ et avoir éliminé entre elles $\beta - a'$.

Mais on a vu plus haut que ces équations donnent

$$(\alpha - a)^2 + (\alpha' - b)^2 = r^2$$

et

$$(\beta - a')^2 + (\beta' - b')^2 = r'^2.$$

Il suffira donc de faire dans celles-ci $\beta' = 0$ et d'y remplacer $\beta - a'$ par $-b'\frac{\alpha - a}{\alpha' - b}$.

On en tire alors

$$\alpha' - b = \pm\frac{rb'}{r'}$$

et

$$(\alpha - a) = \pm\frac{r}{r'}\sqrt{r'^2 - b'^2}.$$

En substituant dans les expressions de $\frac{dy_1}{dx_1}$ et de $\frac{d^2y_1}{dx_1^2}$, il vient

$$\frac{dy_1}{dx_1} = \pm\frac{\sqrt{r'^2 - b'^2}}{b'}$$

et

$$\frac{d^2y_1}{dx_1^2} = -\frac{r^2}{\frac{r^2b'^2}{r'^2}\left(\frac{r^2b'^2}{r'^2} + b'^2\right)}\left(b' \pm \frac{rb'}{r'}\right) = -\frac{r'^3(r' \pm r)}{b'^3(r^2 + r'^2)}.$$

Par conséquent le rayon de courbure cherché serait

$$\mathrm{R} = \pm\frac{\left(1 + \frac{r'^2 - b'^2}{b'^2}\right)^{\frac{3}{2}}}{\frac{r'^3(r' \pm r)}{b'^3(r^2 + r'^2)}} = \pm\left(\frac{r^2 + r'^2}{r' \pm r}\right).$$

**143.** Mais il est impossible d'admettre concurremment pour $R^2$ les deux valeurs qu'on vient de trouver. En effet, chaque conjuguée qui touche l'enveloppe la touche bien en deux points, mais ce ne pourrait être, en tous cas, à cette circonstance que fût due l'ambiguïté qui affecte $R^2$, puisque la conjuguée ayant pour axe de symétrie un diamètre de l'enveloppe elle-même, les deux points de contact doivent être symétriques l'un de l'autre et la conjuguée doit y avoir même courbure.

L'ambiguïté du double signe qui se trouve dans la valeur de $R^2$ tient à une autre cause. Si l'on reprend les équations (1), (2), (3) :

$$(1) \quad (\alpha - a)^2 - (\beta - a')^2 + (\alpha' - b)^2 - (\beta' - b')^2 = r^2 - r'^2,$$

$$(2) \quad (\alpha - a)(\beta - a') + (\alpha' - b)(\beta' - b') = rr'$$

et

$$(3) \quad \frac{\alpha - a}{\alpha' - b} = \frac{\beta - a'}{\beta' - b'},$$

on voit que les deux dernières seules établissent de certaines dépendances entre les signes des quantités $\alpha - a$, $\alpha' - b$, $\beta - a'$ et $\beta' - b'$. Or l'équation (3) montre que les produits

$$(\alpha - a)(\beta - a') \quad \text{et} \quad (\alpha' - b)(\beta' - b')$$

sont toujours de même signe, et l'équation (2) ensuite exige qu'ils aient le signe de $rr'$.

Dans le cas donc où $r$ et $r'$ auront le même signe, $\alpha' - b$ et $\beta' - b'$ devront aussi être de même signe, et par conséquent si l'on a supposé que $\beta'$ fût nul, ce qui aura réduit $\beta' - b'$ à $-b'$, bien qu'on ait trouvé pour $\alpha' - b$ la valeur

$$\alpha' - b = \pm \frac{rb'}{r'},$$

on ne devra prendre que la valeur

$$\alpha' - b = -\frac{rb'}{r'},$$

et si $r$ et $r'$ sont de signes contraires, $\alpha' - b$ et $\beta' - b'$ devant être aussi de signes contraires, on devra prendre encore

$$\alpha' - b = -\frac{rb'}{r'}.$$

Ainsi $\alpha' - b$ ne doit jamais recevoir que la seule valeur

$$\alpha' - b = -\frac{rb'}{r'},$$

d'où il résulte que $R^2$ en réalité se réduit à

$$R^2 = \left(\frac{r^2 + r'^2}{r - r'}\right)^2.$$

**144.** Quant au centre de courbure, il se trouve naturellement sur la normale à l'enveloppe, mais rien, dans ce qui précède, ne prouve qu'il doive être plutôt d'un côté que de l'autre du point de contact.

Pour trancher la question, il faut calculer l'une au moins des coordonnées de ce centre. Nous allons en déterminer l'$y$.

L'ordonnée réalisée du centre de courbure est

$$y_1 + \frac{1 + \left(\frac{dy_1}{dx_1}\right)^2}{\frac{d^2y_1}{dx_1^2}}.$$

Or les formules précédentes donnent

$$\frac{1 + \left(\frac{dy_1}{dx_1}\right)^2}{\frac{d^2y_1}{dx_1^2}} = -\frac{b'(r^2 + r'^2)}{r'(r' - r)};$$

quant à $y_1$, qui se réduit à $\alpha'$, puisque $\beta'$ est nul, sa valeur est fournie par l'équation

$$\alpha' - b = -\frac{rb'}{r'},$$

qui donne

$$y_1 = \alpha' = \frac{br' - rb'}{r'}.$$

Cela posé, il s'agit de savoir si le centre de courbure de la conjuguée du cercle imaginaire au point où elle touche son enveloppe est, par rapport à ce point, du même côté que le centre de courbure de l'enveloppe ou du côté opposé : cela se réduit à savoir si les différences des ordonnées du point de l'enveloppe et des deux centres sont de même signe ou de signes contraires, c'est-à-dire si

$$y_1 + \frac{1+\left(\frac{dy_1}{dx_1}\right)^2}{\frac{d^2y_1}{dx_1^2}} - y_1$$

et

$$b + b' - y_1$$

sont de même signe ou de signes contraires. Or ces différences se réduisent à

$$-\frac{b'(r^2+r'^2)}{r'(r'-r)} \quad \text{et} \quad \frac{b'(r'+r)}{r'}$$

dont le quotient est

$$\frac{r^2+r'^2}{r^2-r'^2};$$

de sorte que selon que $r^2 - r'^2$ sera positif ou négatif, le centre de courbure de la conjuguée sera, par rapport au point où elle touche l'enveloppe, du même côté que le centre de courbure de cette enveloppe ou du côté opposé.

**145.** Tous les calculs qui précèdent se rapportaient à la conjuguée $C = 0$ du cercle imaginaire

$$(x - a - a'\sqrt{-1})^2 + (y - b - b'\sqrt{-1})^2 = (r + r'\sqrt{-1})^2.$$

mais les résultats auxquels on est parvenu ne contenant aucune des constantes $a$, $a'$, $b$, $b'$ qui seules pourraient changer lorsqu'on changerait les axes, ces résultats conviennent à une conjuguée quelconque.

La forme circulaire de l'enveloppe pouvait permettre de présumer cette permanence dans les résultats, et c'est du reste ce qui a engagé à les chercher.

**146.** On pourra toujours, quand on le voudra, déterminer le centre et le rayon de courbure d'une conjuguée C d'un lieu

$$f(x, y) = 0$$

en un de ses points, au moyen des parties réelles et imaginaires des coordonnées

$$x = \alpha + \beta\sqrt{-1},$$
$$y = \alpha' + \beta C\sqrt{-1}$$

de ce point et des éléments $a$, $b$, $a'$, $b'$, $r$, $r'$ du cercle osculateur au lieu en ce point.

L'équation en coordonnées réelles de la conjuguée C du cercle osculateur

$$(x - a - a'\sqrt{-1})^2 + (y - b - b'\sqrt{-1})^2 = (r + r'\sqrt{-1})^2$$

sera en effet fournie par le système

$$x = \alpha + \beta, \quad y = \alpha' + \beta C,$$
$$(\alpha - a)^2 - (\beta - a')^2 + (\alpha' - b)^2 - (\beta C - b')^2 = r^2 - r'^2,$$
$$(\alpha - a)(\beta - a')^2 + (\alpha' - b)(\beta C - b') = rr',$$

qui permettra d'obtenir $\frac{dy}{dx}$ et $\frac{d^2y}{dx^2}$ au moyen de $\frac{d\beta}{d\alpha}$, $\frac{d\alpha'}{d\alpha}$, $\frac{d^2\beta}{d\alpha^2}$ et $\frac{d^2\alpha'}{d\alpha^2}$ qu'on pourra exprimer d'autre part en fonction de $\alpha$, $\alpha'$ et $\beta$.

Ainsi la solution pratique de la question ne sera jamais difficile à obtenir. Mais il est clair qu'une pareille solution, capable seulement de fournir les valeurs numériques des résultats dans chaque cas, ne saurait conduire à la constatation d'aucune loi.

La courbure d'une courbe en un de ses points est un angle : si la courbe est imaginairement représentée, sa courbure doit l'être aussi, sans quoi toute comparaison, tout rapprochement deviennent impossibles.

La théorie des courbures des courbes imaginaires nécessite donc l'introduction d'angles imaginaires.

## SUR LA FORME
## $x^2 + 2y^2 + 4z^2 + 8t^2$;
### PAR M. J. LIOUVILLE.

1. J'ai déjà eu l'occasion de faire observer que la forme

$$x^2 + 2y^2 + 4z^2 + 8t^2$$

peut servir à représenter tous les nombres. Mais il s'agit ici d'indiquer une regle simple qui permette de calculer à priori, pour chaque entier donné $n$, le nombre exact N des représentations, c'est-à-dire le nombre N des solutions de l'équation indéterminée

$$n = x^2 + 2y^2 + 4z^2 + 8t^2,$$

où $x$, $y$, $z$, $t$ sont des entiers indifféremment positifs, nuls ou négatifs.

Comme $n$ peut être tantôt pair et tantôt impair, je ferai

$$n = 2^{\alpha} m,$$

$m$ étant impair et l'exposant $\alpha$ pouvant se réduire à zéro.

Le cas de $n$ pair est le plus simple. Il se subdivise à la vérité en quatre autres; mais N n'y dépend jamais que de la somme $\zeta_1(m)$ des diviseurs de $m$, et se rattache facilement au nombre des représentations de $n$ par une somme de quatre carrés. Le cas de $n$ impair (du moins pour un nombre de la forme $4\mu + 1$) exige au contraire qu'on adjoigne à $\zeta_1(m)$ une fonction numérique nouvelle.

2. Commençons donc par prendre $n$ pair, et soit d'abord $n$ impairement pair, $n = 2m$. Je trouve qu'on aura alors

$$\mathrm{N} = 2\zeta_1(m).$$

Ainsi pour $m = 1$, $n = 2$, on a

$$N = 2,$$

et c'est ce que confirme l'équation

$$2 = 0^2 + 2(\pm 1)^2 + 4.0^2 + 8.0^2$$

qui fournit en effet deux représentations.

Soit encore $m = 3$, $n = 6$; il viendra

$$N = 2.4 = 8,$$

ce qui est exact, puisque l'on a

$$6 = (\pm 2)^2 + 2(\pm 1)^2 + 4.0^2 + 8.0^2,$$

et

$$6 = 0^2 + 2(\pm 1)^2 + 4(\pm 1)^2 + 8.0^2.$$

Soit enfin $m = 5$, $n = 10$, d'où

$$N = 2.6 = 12:$$

la vérification cherchée sera fournie cette fois par les équations

$$10 = (\pm 2)^2 + 2(\pm 1)^2 + 4(\pm 1)^2 + 8.0^2$$

et

$$10 = 0^2 + 2(\pm 1)^2 + 4.0^2 + 8(\pm 1)^2.$$

Il serait inutile de pousser plus loin ces calculs.

5. Soit, en second lieu, $n$ divisible par 4, mais non par 8, $n = 4m$. La valeur de N deviendra

$$N = 4\zeta_1(m).$$

Ainsi pour $m = 1$, $n = 4$, on devra avoir

$$N = 4;$$

or c'est ce que confirment les deux équations

$$4 = (\pm 2)^2 + 2.0^2 + 4.0^2 + 8.0^2$$

et

$$4 = 0^2 + 2.0^2 + 4(\pm 1)^2 + 8.0^2.$$

Soit encore $m = 3$, $n = 12$. Notre formule donnera

$$N = 4.4 = 16;$$

or il existe en effet seize représentations, vu que l'on a

$$12 = (\pm 2)^2 + 2(\pm 2)^2 + 4.0^2 + 8.0^2$$

et

$$12 = 0^2 + 2(\pm 2)^2 + 4(\pm 1)^2 + 8.0^2,$$

puis

$$12 = (\pm 2)^2 + 2.0^2 + 4.0^2 + 8(\pm 1)^2,$$

enfin

$$12 = 0^2 + 2\,0^2 + 4(\pm 1)^2 + 8(\pm 1)^2.$$

On continuera aisément, si l'on veut, ces vérifications.

4. Soit à présent $n$ divisible par 8, non par 16, $n = 8m$. J'obtiens alors

$$N = 8\zeta_1(m).$$

Ainsi pour $m = 1$, $n = 8$, on devra avoir

$$N = 8,$$

et c'est ce qui résulte effectivement des trois équations

$$8 = (\pm 2)^2 + 2.0^2 + 4(\pm 1)^2 + 8.0^2,$$
$$8 = 0^2 + 2(\pm 2)^2 + 4.0^2 + 8.0^2,$$
$$8 = 0^2 + 2.0^2 + 4.0^2 + 8(\pm 1)^2.$$

Soit encore $m = 3$, $n = 24$. Il faudra que

$$N = 8.4 = 32.$$

Or, je vois que l'on a d'une part

$$24 = (\pm 4)^2 + 2(\pm 2)^2 + 4.0^2 + 8.0^2,$$

puis

$$24 = 0^2 + 2(\pm 2)^2 + 4(\pm 2)^2 + 8.0^2,$$

et d'autre part

$$24 = (\pm 4)^2 + 2.0^2 + 4.0^2 + 8(\pm 1)^2,$$

puis

$$24 = 0^2 + 2.0^2 + 4(\pm 2)^2 + 8(\pm 1)^2,$$

enfin

$$24 = (\pm 2)^2 + 2(\pm 2)^2 + 4(\pm 1)^2 + 8(\pm 1)^2,$$

ce qui fournit bien les trente-deux représentations annoncées.

5. Prenons maintenant $n$ divisible par 16, ou généralement $n = 2^\alpha m$, avec $\alpha = 4$ ou $\alpha > 4$. La valeur de N, si grand que soit $\alpha$, restera toujours

$$N = 24\zeta_1(m),$$

comme dans le théorème de Jacobi pour le nombre des représentations d'un entier pair en une somme de quatre carrés.

Ainsi, pour $m = 1$, $\alpha = 4$, $n = 16$, on aura

$$N = 24.$$

Les équations qui fournissent les vingt-quatre représentations indiquées sont, d'une part

$$16 = (\pm 4)^2 + 2.0^2 + 4.0^2 + 8.0^2,$$

puis

$$16 = 0^2 + 2.0^2 + 4(\pm 2)^2 + 8.0^2$$

et

$$16 = (\pm 2)^2 + 2(\pm 2)^2 + 4(\pm 1)^2 + 8.0^2,$$

d'autre part

$$16 = 0^2 + 2(\pm 2)^2 + 4.0^2 + 8(\pm 1)^2$$

et

$$16 = (\pm 2)^2 + 2.0^2 + 4(\pm 1)^2 + 8(\pm 1)^2.$$

Soit ensuite $m = 1$, mais $\alpha = 5$, $n = 32$, et l'on devra continuer à avoir

$$N = 24.$$

C'est ce qui arrive, les équations qui fournissent les représentations de 32 étant

$$32 = 0^2 + 2(\pm 4)^2 + 4.0^2 + 8.0^2,$$
$$32 = (\pm 4)^2 + 2.0^2 + 4(\pm 2)^2 + 8.0^2,$$
$$32 = (\pm 4)^2 + 2(\pm 2)^2 + 4.0^2 + 8(\pm 1)^2,$$
$$32 = 0^2 + 2(\pm 2)^2 + 4(\pm 2)^2 + 8(\pm 1)^2,$$
$$32 = 0^2 + 2.0^2 + 4.0^2 + 8(\pm 2)^2.$$

6. Soit enfin $n$ impair, $n = m$. Il faudra alors considérer les décompositions dont $m$ est susceptible sous la forme

$$m = i^2 + 4s^2,$$

$i$ étant un entier impair et positif, tandis que l'entier $s$ est indifféremment positif, nul ou négatif. On distinguera les valeurs de $i$ qui sont de la forme $4k+1$ et celles qui sont de la forme $4k+3$. L'excès de la somme des premières sur la somme des dernières, que l'on peut représenter par

$$\sum (-1)^{\frac{i-1}{2}} i,$$

constitue une fonction nouvelle qu'il faudra tantôt ajouter à $\zeta_1(m)$, tantôt retrancher de $\zeta_1(m)$, pour avoir dans le cas de $n$ impair $(n = m)$ que nous discutons la valeur de N. La formule générale est

$$N = \zeta_1(m) + (-1)^{\frac{m^2-1}{8}} \sum (-1)^{\frac{i-1}{2}} i.$$

Quand $m$ est de la forme $4\mu + 3$, l'équation

$$m = i^2 + 4s^2$$

est impossible, de sorte qu'il vient simplement

$$N = \zeta_1(m),$$

sans fonction numérique nouvelle.

Ainsi, pour $n = m = 3$, on a

$$N = \zeta_1(3) = 4,$$

ce qui est vérifié par l'équation

$$3 = (\pm 1)^2 + 2(\pm 1)^2 + 4.0^2 + 8.0^2.$$

De même, pour $n = m = 7$, on doit avoir

$$N = \zeta_1(7) = 8.$$

L'équation

$$7 = (\pm 1)^2 + 2(\pm 1)^2 + 4(\pm 1)^2 + 8.0^2$$

confirme ce fait.

Quand $m$ est de la forme $4\mu + 1$, l'équation

$$m = i^2 + 4s^2$$

est souvent possible, et quand elle a réellement lieu, l'intervention de la fonction numérique

$$\sum (-1)^{\frac{i-1}{2}} i$$

devient nécessaire. Il faut, pour avoir N, ajouter la valeur de cette fonction à celle de $\zeta_1(m)$, ou la retrancher, suivant que l'on a

$$(-1)^{\frac{m^2-1}{8}} = 1,$$

ou, au contraire,

$$(-1)^{\frac{m^2-1}{8}} = -1,$$

c'est-à-dire suivant que $m$ est de la forme $8g+1$ ou de la forme $8g+5$.

Ainsi, pour $m = 8g + 1$, on a

$$N = \zeta_1(m) + \sum (-1)^{\frac{i-1}{2}} i.$$

Soit, comme exemple, le nombre $1 = 1^2 + 4.0^2$. On aura

$$N = 1 + 1 = 2,$$

ce qui s'accorde avec l'équation

$$1 = (\pm 1)^2 + 2.0^2 + 4.0^2 + 8.0^2.$$

Soit, comme second exemple, le nombre $9 = 3^2 + 4.0^2$. Il faudra que

$$N = \zeta_1(9) - 3 = 10.$$

Les équations ci-après

$$9 = (\pm 3)^2 + 2.0^2 + 4.0^2 + 8.0^2,$$
$$9 = (\pm 1)^2 + 2(\pm 2)^2 + 4.0^2 + 8.0^2,$$
$$9 = (\pm 1)^2 + 2.0^2 + 4.0^2 + 8(\pm 1)^2,$$

confirment ce fait.

Pour $m = 8g + 5$ on aura, au contraire,

$$N = \zeta_1(m) - \sum (-1)^{\frac{i-1}{2}} i.$$

Soit, comme exemple, le nombre 5. Comme on a

$$5 = 1^2 + 4(\pm 1)^2,$$

il y a ici deux valeurs de $i$, l'une et l'autre égales à 1, en sorte que

$$N = 6 - 2 = 4.$$

Les quatre décompositions que la formule indique répondent à l'équation

$$5 = (\pm 1)^2 + 2.0^2 + 4(\pm 1)^2 + 8.0^2,$$

et il est clair qu'il n'y en a pas d'autres.

7. Nous savons d'avance que tout entier $n$, pair ou impair, peut s'exprimer par la forme

$$x^2 + 2y^2 + 4z^2 + 8t^2.$$

Mais il est bon de montrer que cela résulte des équations que nous venons de donner pour calculer N dans chaque cas. La difficulté, s'il y en a une, ne peut concerner que les nombres impairs $4\mu+1$. Il faut prouver que pour eux on a toujours

$$\zeta_1(m)+(-1)^{\frac{m^2-1}{8}}\sum(-1)^{\frac{i-1}{2}}i>0.$$

Or, je dis qu'en laissant de côté le cas vérifié déjà de $m=1$, l'on a même

$$\zeta_1(m)>\sum i.$$

En effet soit $j$ le plus grand entier impair contenu dans $\sqrt{m}$. L'équation $m=i^2+4s^2$, où chaque valeur convenable de $i$ ne peut être employée que deux fois au plus, entraîne l'inégalité

$$\sum i \leqq 2(1+3+5+\ldots+j),$$

d'où

$$\sum i \leqq \frac{1}{2}(j+1)^2,$$

ce qui donne toujours

$$\sum i<\frac{1}{2}(m+2\sqrt{m}+1),$$

attendu que la valeur $i=\sqrt{m}$, qu'on doit compter quand $m$ est un carré $j^2$, ne peut être employée qu'une fois, $s$ se réduisant alors à zéro. Mais d'un autre côté $\zeta_1(m)$ est au moins égal à $m+1$. La différence

$$m+1-\frac{1}{2}(m+2\sqrt{m}+1)=\frac{m-2\sqrt{m}+1}{2}$$

est d'ailleurs positive dès $m=5$. Notre démonstration est donc complète. On voit en outre que quand $m$ augmente à l'infini, N augmente pareillement à l'infini.

# MÉMOIRE

SUR

# LA THÉORIE GÉNÉRALE DES PERMUTATIONS;

Par M. DESPEYROUS,

Professeur à la Faculté des Sciences de Dijon.

## INTRODUCTION.

Les phénomènes périodiques étant les plus nombreux dans la nature, il doit être intéressant d'étudier *l'ordre périodique indépendamment de toute considération de grandeur* : « théorie, dit Poinsot [*], » neuve et profonde dont les éléments sont à peine connus, mais » qu'on doit regarder comme le premier fondement de l'algèbre et la » source naturelle des principales propriétés des nombres. »

D'ailleurs cette théorie se rattache à d'autres considérations dont nous parlerons dans une autre circonstance, considérations qui simplifieront notablement plusieurs théories importantes et feront naître des résultats nouveaux.

La théorie de l'ordre périodique est une géométrie spéciale qui ne considère que la situation des choses, la disposition des lieux dans l'espace et fait partie de la *géométrie de position* entrevue par Leibniz.

Cette théorie fait retrouver les polygones étoilés [**] de Poinsot et fournit une méthode très-directe pour partager toutes les permutations d'un nombre quelconque de lettres en plusieurs groupes de permutations associées de telle manière, que, malgré tous les échanges qu'on voudrait faire de ces lettres, les permutations d'un même groupe ne puissent jamais se séparer; pour constituer avec ces derniers groupes de permutations d'autres groupes de permutations également insépa-

[*] *Mémoires de l'Institut pour les années* 1813, 1814, 1815, p 382.

[**] *Journal de l'École Polytechnique*, X$^e$ cahier, p. 16.

rables, et ainsi de suite pour les groupes successifs obtenus qui se subdivisent d'après *certains* diviseurs du nombre total des permutations.

La même méthode partage les racines de toute *équation abélienne* [*] en plusieurs groupes de racines *inséparables*, quel que soit l'échange que l'on considère, associe ces groupes eux-mêmes en de nouveaux groupes de racines également inséparables, et ainsi de suite pour les groupes successifs obtenus qui se subdivisent d'après *tous* les diviseurs du degré de l'équation.

Telles sont les deux lois générales de classification que notre travail démontre. Le profond géomètre dont nous avons déjà parlé, Poinsot, avait, dès l'année 1817, entrevu une partie de ces résultats, et avait promis sur cette matière plusieurs Mémoires. Les géomètres regretteront sans doute qu'il n'ait pas réalisé sa promesse : loin de nous la prétention d'y suppléer. Mais nous croyons avoir trouvé deux lois importantes et nous les soumettons au jugement des géomètres.

Le rapprochement de la première de ces deux lois du théorème général de Lagrange relatif au nombre de valeurs que peut acquérir une fonction par les permutations des lettres qu'elle renferme, ce rapprochement, dis-je, fait naître la pensée que cette loi offrira des ressources nouvelles à la solution de cette double question d'abord mise au concours pour le grand prix des sciences mathématiques de l'année 1860 et puis retirée au mois de mars dernier : « 1° Quel est le nombre de valeurs que peut acquérir une fonction par les permutations des lettres qu'elle renferme ; 2° comment peut-on former les fonctions primitives pour lesquelles les nombres de valeurs distinctes soient les nombres trouvés. »

C'est effectivement ce que nous démontrerons dans une autre occa-

---

[*] Une équation est dite *abélienne* lorsque ses $n$ racines $x_1, x_2, x_3, \ldots, x_n$ sont telles, que

$$x_2 = \theta(x_1), \quad x_3 = \theta(x_2), \ldots, \quad x_n = \theta(x_{n-1}), \quad x_1 = \theta(x_n),$$

$\theta$ désignant une fonction rationnelle.

Cette dénomination tire son nom du célèbre géomètre Abel, qui le premier a étudié cette classe d'équations à laquelle il a été conduit en généralisant une idée de Gauss.

sion. Nous prouverons aussi que la deuxième loi démontrée dans notre Mémoire permet d'établir, en quelques lignes et de la manière la plus simple, les beaux théorèmes de Gauss et d'Abel sur la résolution des équations binômes et en général sur celle des équations abéliennes. Enfin nous ferons connaître les résultats indiqués seulement par Poinsot et les résultats nouveaux que produit l'application de ces deux lois à la théorie générale des équations.

## I.

### *Suites périodiques.*

Considérons une suite périodique et indéfinie dans les deux sens

(1) $$\ldots abc,\ldots kl,\; abc\ldots kl,\; abc\ldots kl,\ldots$$

dont la période est composée d'un nombre quelconque de lettres marqué par $n$, $a$, $b$, $c$,..., $k$, $l$ écrites dans un ordre déterminé, $abc\ldots kl$ par exemple, et examinons, s'il est possible, en prenant les lettres de cette suite par *intervalles constants* à partir de la première $a$, de déduire de cette suite périodique d'autres suites également périodiques, la période étant composée des *mêmes* lettres, mais dans un ordre différent.

D'abord en prenant les lettres de cette suite (1) successivement, on retrouve cette suite qui satisfait aux conditions énoncées, et si nous les prenons à partir de $a$ de $p$ en $p$, $p$ étant un sous-multiple de $n$, $pq = n$, il est clair qu'on ne prendra de chaque période que $q$ lettres, et que par suite on aura une nouvelle suite périodique qui ne satisfera pas aux conditions dônnées, puisque la période se composera seulement de $q$ lettres.

Mais si nous prenons les lettres de la suite (1) à partir de la première $a$, de $p$ en $p$, et si $p$ est premier à $n$, je dis qu'on obtiendra une nouvelle suite satisfaisant à toutes les conditions demandées.

En effet, à partir de la lettre $a$ de l'une quelconque des périodes de la suite (1) prenons, en marchant toujours de gauche à droite, les lettres de cette suite de $p$ en $p$. Nous retomberons nécessairement sur la lettre $a$ de départ après avoir parcouru $p$ périodes consécutives, puisque $p$ est un sous-multiple du nombre $pn$ de lettres qui entrent dans

ces $p$ périodes consécutives, et par suite nous formerons une nouvelle suite périodique. Il y a plus : nous prendrons les $n$ lettres données avant de retomber pour la première fois sur cette lettre $a$ : car les rangs des lettres d'une période quelconque $abc \ldots kl$ étant respectivement désignés par $0, 1, 2, 3, \ldots, n-1$, et ceux des lettres des périodes suivantes par $n$, $n+1$, $n+2$, etc., nous prendrons, en marchant de $p$ en $p$, les lettres de ces $p$ périodes consécutives dont les rangs sont marqués par les multiples

$$p,\ 2p,\ 3p, \ldots,\ (n-1)p;$$

et par conséquent les lettres de la *première* période dont les rangs sont marqués par les résidus à $n$ de ces mêmes multiples.

Or $p$ étant premier à $n$, ces $n-1$ résidus sont différents les uns des autres et aucun d'eux n'est nul. Car si l'un quelconque de ces multiples $kp$, $k$ étant un nombre entier inférieur à $n$, avait pour résidu à $n$ zéro, $kp$ serait égal à un multiple de $n$, ce qui est absurde, puisque $p$ est premier à $n$ et $k$ inférieur à $n$. De même si deux quelconques de ces mêmes multiples $kp$, $k'p$ avaient leurs résidus à $n$ égaux entre eux, leur différence $(k-k')p$ serait égal à un multiple de $n$, ce qui ne peut être, puisque $p$ est premier à $n$ et $k-k'$ inférieur à $n$. Ces $n-1$ résidus étant différents et aucun d'eux ne pouvant être nul, seront égaux, dans un ordre déterminé, aux nombres $1, 2, 3, \ldots, n-1$. Donc la période de la nouvelle suite formée se compose des $n$ lettres données, et, par suite, en prenant les lettres de la suite (1) de $p$ en $p$, $p$ étant inférieur et premier à $n$, on formera une nouvelle suite périodique, la période commençant par $a$ et étant composée des $n$ lettres données. De là ce premier théorème :

THÉORÈME I. — *Si $p_1, p_2, p_3, \ldots, p_\nu$ désignent les $\nu$ nombres inférieurs et premiers à $n$, parmi lesquels se trouvent l'unité et $n-1$, on peut, avec $n$ lettres écrites dans un ordre déterminé mais quelconque, former $\nu$ [*] suites périodiques, la période de chacune d'elles commençant par la première et composée des mêmes $n$ lettres.*

---

[*] Si $n = a^\alpha b^\beta c^\gamma \ldots k^\delta$, on sait que

$$\nu = a^{\alpha-1} b^{\beta-1} c^{\gamma-1} \ldots k^{\delta-1} . (a-1)(b-1)(c-1) \ldots (k-1).$$

*Remarque.* — Si $p_i$ est premier à $n$, $n - p_i$ sera aussi premier à $n$ : donc si $p_i$ fournit la période *abl... ch*, $n - p_i$ fournira la période *ahc... lb*. De là il suit que les $\nu$ périodes peuvent être partagées en deux groupes composés chacun de $\frac{\nu}{2}$ périodes telles, que chaque période appartenant à l'un des groupes ne soit autre que l'une des périodes de l'autre groupe lue à l'envers.

*Premier exemple :* $n = 4$, auquel cas $\nu = 2$, $p_1 = 1$, $p_2 = 3$. Donc la disposition *abcd* produira les deux suites périodiques

*...abcd, abcd, abcd,...*
*...adcb, adcb, adcb,...*

*Second exemple :* Pour $n = 5$, on aura $p_1 = 1$, $p_2 = 2$, $p_3 = 3$, $p_4 = 4$, $\nu = 4$, et par suite les quatre suites relatives à la disposition *abcde* :

*...abcde, abcde, abcde,...*
*...acebd, acebd, acebd,...*
*...adbec, adbec, adbec,...*
*...aedcb, aedcb, aedcb,...*

Ces deux exemples suffisent pour les applications de ce premier théorème.

Théorème II. — *Le nombre de suites périodiques qu'on peut former par la loi précédente avec n lettres écrites dans tel ordre qu'on voudra, les périodes étant composées de ces lettres et commençant toutes par la première, est égal au nombre $\nu$ qui marque combien il y a de nombres inférieurs et premiers à ce nombre de lettres.*

En effet, le premier théorème démontre qu'on peut en former $\nu$, il suffit donc de prouver qu'il n'y en a pas d'autres.

D'abord si nous répétons indéfiniment la permutation donnée qu'offrent ces $n$ lettres, nous aurons une première suite périodique satisfaisant aux conditions énoncées. Mais l'intervalle constant $p$, par lequel on doit sauter d'une lettre à une autre, pour déduire de cette suite une nouvelle satisfaisant aux mêmes conditions, devant être inférieur à $n$, il ne pourra arriver que trois cas :

1° Cet intervalle constant $p$ est un sous-multiple de $n$, et alors la suite périodique, déduite de la suite donnée (1), ne remplira pas les conditions énoncées.

2° Cet intervalle constant $p$ est premier à $n$, et alors la suite obtenue satisfera aux conditions prescrites.

3° Enfin cet intervalle constant $p$ aura avec $n$ un plus grand commun diviseur $\theta$, et alors si l'on pose

$$p = p'\theta, \quad n = n'\theta,$$

$p'$ et $n'$ seront premiers entre eux. Or si l'on prend les lettres de la suite (1) de $\theta$ en $\theta$ à partir de la première $a$, nous obtiendrons une nouvelle suite périodique dont la période commencera par $a$ et sera formée de $n'$ lettres seulement; et si dans cette nouvelle suite nous prenons les lettres à partir de $a$ de $p'$ en $p'$, nous obtiendrons, $p'$ étant premier à $n'$, une troisième suite périodique dont la période commencera par $a$ et sera formée de $n'$ lettres. Mais prendre dans la suite (1) les lettres à partir de $a$, d'abord de $\theta$ en $\theta$ et puis de $p'$ en $p'$ dans le résultat obtenu, c'est évidemment prendre dans la suite (1) les lettres à partir de $a$ de $\theta p'$ en $\theta p'$, c'est-à-dire de $p$ en $p$, et comme cette troisieme suite ne contient que $n'$ des $n$ lettres données, elle ne satisfait pas aux conditions énoncées.

Il n'y a donc qu'une seule manière de déduire, par intervalle constant, d'une suite périodique donnée une nouvelle suite périodique dont la période commence par la même lettre que dans la période donnée et soit formée des mêmes lettres. Cette manière consite à prendre pour intervalle constant un nombre quelconque inférieur et premier au nombre de lettres données, ce qui, d'après le premier théoreme, démontre le second.

*Corollaire I.* — Il résulte évidemment de là que les $\nu$ suites dont il est question dans le premier théorème sont *rentrantes* sur elles-mêmes; c'est-à-dire que, l'une d'elles étant donnée, on en déduira, par le procédé de l'intervalle constant, les mêmes $\nu$ suites.

Considérons en effet l'une d'elles, celle qui est produite par le

nombre $p_i$ par exemple, et marchons dans cette suite de $p_h$ en $p_h$. Marcher dans la suite (1) d'abord de $p_i$ en $p_i$ et puis dans la suite produite de $p_h$ en $p_h$, c'est évidemment marcher dans la suite (1) de $p_i . p_h$ en $p_i . p_h$ Or $n$ étant premier à $p_i$ et à $p_h$ sera premier à leur produit $p_i . p_h$ et le résidu à $n$ de $p_i . p_h$ sera aussi premier à $n$; donc ce résidu sera l'un des $\nu$ nombres $p_1$, $p_2, \ldots, p_\nu$, et par conséquent la suite ainsi obtenue coïncidera avec l'une des $\nu$ suites du premier théorème.

*Corollaire II.* — Si $n$ a des racines *primitives*, c'est-à-dire si $n$ est égal à un nombre premier quelconque supérieur à 2, ou à une puissance d'un nombre premier (excepté si $n = 2^\alpha$ et $\alpha > 2$), ou enfin au double d'un nombre premier élevé à un puissance quelconque, on peut obtenir les $\nu$ suites du premier théorème en sautant toujours d'un *même* intervalle.

Soit en effet $\rho$ l'une des racines primitives de $n$, les résidus à $n$ de la suite des puissances

$$\rho, \rho^2, \rho^3, \ldots, \rho^\nu$$

seront tous différents et ne seront autres que les $\nu$ nombres inférieurs et premiers à $n$. Si donc, ayant d'abord écrit les $n$ lettres données dans un ordre quelconque, on prend ces lettres de $\rho$ en $\rho$ à partir de la première écrite, on aura, en écrivant le résultat indéfiniment, une première suite satisfaisant aux conditions requises, puisque $\rho$ est premier à $n$. Et si sur cette suite on prend encore les lettres à partir de la première de $\rho$ en $\rho$, ce qui revient évidemment à prendre les lettres de la suite donnée de $\rho^2$ en $\rho^2$ si $\rho^2 < n$ ou de $p_i$ en $p_i$ si $\rho^2 > n$, $p_i$ étant le résidu à $n$ de $\rho^2$, on aura une deuxième suite périodique ayant les conditions énoncées. De même en prenant sur cette dernière suite et à partir de la première les lettres de $\rho$ en $\rho$, on aura une nouvelle suite et ainsi indéfiniment. Donc, d'après le deuxième théorème, on formera ainsi les $\nu$ suites du premier.

*Polygones étoilés* — Plaçons sur une circonférence de rayon quelconque et d'une manière régulière ou irrégulière les $n$ lettres données $a, b, c, \ldots, k, l$ qui forment la période de la suite (1), et traçons le polygone régulier ou irrégulier de $n$ côtés $abc \ldots kl$. Il est clair que ce po-

lygone lu un nombre indéfini de fois dans le même sens sera une représentation géométrique très-exacte de cette suite (1).

Généralement, si $p_i$ est un nombre inférieur et premier à $n$ et si à partir du point $a$ on joint ces $n$ points $a, b, c, \ldots, k, l$ de $p_i$ en $p_i$, le nouveau polygone de $n$ côtés obtenu, lu indéfiniment dans le même sens, représentera celle des $\nu$ suites du premier théorème relative à ce nombre $p_i$.

Il faut remarquer que puisque $p_i$ périodes consécutives de la suite (1) sont nécessaires pour former la période de la suite relative à $p_i$, le polygone de $n$ côtés qui remplace cette suite s'obtiendra en partant du point $a$ et faisant $p_i$ fois le tour de la circonférence.

De là et des théorèmes I et II, ce théorème dû à Poinsot :

Théorème III. — *Avec $n$ points régulièrement ou irrégulièrement espacés sur une circonférence, on ne peut former qu'un nombre $\nu$ de polygones réguliers ou irréguliers de $n$ côtés marqué par le nombre qui exprime combien il y a de nombres inférieurs et premiers à ce nombre $n$ de points donnés.*

*Corollaire.* — La remarque du premier théorème démontre qu'il y a $\frac{\nu}{2}$ polygones qu'on obtient en marchant dans un sens sur la circonférence et $\frac{\nu}{2}$ autres qui ne sont autres que les $\frac{\nu}{2}$ premiers lus en sens inverse.

*Remarque.* — A peine est-il besoin d'ajouter que les $n$ points donnés auraient pu être portés sur toute autre courbe fermée que la circonférence de cercle : mais alors il faudrait effacer en général le mot *régulier*.

*Note.* — Le profond géomètre dont il est ici question a déduit de son théorème plusieurs conséquences remarquables : on les trouvera dans le Mémoire déjà cité du *Journal de l'École Polytechnique* et dans le tome X du *Journal de Mathématiques* publié par M. Liouville.

Nous terminerons cette première section par un *nouveau* théorème qui nous sera utile dans la recherche des équations solubles par radicaux.

THÉORÈME IV. — *Si $\rho$ est une des racines primitives du nombre entier $n$, et si $p_i$ est un des $\nu$ nombres inférieurs et premiers à $n$, les $\nu$ permutations produites par les $\nu$ polygones de Poinsot des $n$ choses $x$, $x_{p_i}$, $x_{2p_i}$, $x_{3p_i}$,..., $x_{(n-1)p_i}$ considérées dans cet ordre, sont*

$$x\ x_{p_i}\ x_{2p_i}\ x_{3p_i}\ldots\ x_{(n-1)p_i},$$
$$x\ x_{p_i\rho}\ x_{2p_i\rho}\ x_{3p_i\rho}\ldots\ x_{(n-1)p_i\rho},$$
$$x\ x_{p_i\rho^2}\ x_{2p_i\rho^2}\ x_{3p_i\rho^2}\ldots\ x_{(n-1)p_i\rho^2},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x\ x_{p_i\rho^{\nu-1}}\ x_{2p_i\rho^{\nu-1}}\ldots\ x_{(n-1)p_i\rho^{\nu-1}},$$

*les indices de $x$ étant pris suivant le module $n$.*

En effet, $p_i$ étant premier à $n$ et $\rho$ étant une racine primitive de ce nombre $n$, aucun des indices de $x$, $p_i\rho^h$, $2p_i\rho^h$, $3p_i\rho^h$,..., $(n-1)p_i\rho^h$ relatifs à une quelconque de ces permutations ne sera divisible par $n$, et de plus je dis que les $n-1$ restes obtenus seront différents. Car si, chacun des nombres $k$, $k'$ étant inférieur à $n$, les restes ou résidus à $n$ de $kp_i\rho^h$ et de $k'p_i\rho^h$ pouvaient être égaux, la différence $k'p_i\rho^h - kp_i\rho^h$ serait un multiple de $n$. On aurait donc, M désignant un nombre entier quelconque,

$$(k'-k)p_i\rho^h = \mathrm{M}.n.$$

Or $n$ divisant le second membre de cette égalité doit diviser le premier; mais $n$ étant premier à $p_i$ et à $\rho$, sera premier au produit $p_i\rho^h$; donc $n$ devrait diviser le facteur $k'-k$, ce qui est impossible, puisque chacun des nombres $k$, $k'$ est inférieur à ce nombre $n$.

1° Donc les résidus à $n$ de tous les indices des termes d'une quelconque des lignes précédentes sont tous différents, et par suite ces résidus ne peuvent être que 1, 2, 3,..., $n-1$ dans tel ou tel ordre.

Les résidus à $n$ des indices des seconds termes dans chacune de ces permutations $p_i$, $p_i\rho$, $p_i\rho^2$,..., $p_i\rho^{\nu-1}$ sont différents aussi, et chacun d'eux est premier à $n$. Car si les résidus à $n$ de $p_i\rho^h$ et de $p_i\rho^{h+h'}$ étaient égaux, chacun des exposants de $\rho$, $h$ et $h+h'$, étant inférieur à $\nu$, la

différence $p_i\rho^{h+k'} - p_i\rho^k$ serait un multiple de $n$, et on aurait

$$p_i\rho^k(\rho^{k'}-1) = \mathrm{M}.n.$$

Or $n$ divisant le second membre de cette égalité doit diviser le premier; mais $n$ est premier au produit $p_i\rho^k$; donc $n$ devrait diviser $\rho^{k'}-1$, ce qui est impossible, puisque $k'$ est inférieur à $\nu$ [*].

Je dis de plus que chacun de ces résidus est premier à $n$; car l'équation

$$p_i\rho^k = \mathrm{M}.n + r$$

prouve que si $r$ et $n$ n'étaient pas premiers entre eux, un quelconque de leurs facteurs premiers communs, $\alpha$ par exemple, divisant le second membre de cette égalité, devrait diviser le premier; et par conséquent diviser ou $p_i$ ou $\rho^k$. Or $\alpha$ ne peut diviser $p_i$, car autrement $n$ et $p_i$ ne seraient pas premiers entre eux; ce facteur $\alpha$ ne saurait non plus diviser $\rho^k$, car, si cela était, $\alpha$ diviserait $\rho$; et par suite $\rho$ et $n$ ne seraient pas premiers entre eux, ce qui ne peut être, puisque $\rho$ est racine primitive de $n$.

2° Donc les résidus à $n$ de $p_i$, $p_i\rho$, $p_i\rho^2,\ldots, p_i\rho^{\nu-1}$ sont tous différents et chacun d'eux est premier à $n$. Ces deux résultats démontrent évidemment le théorème énoncé.

*Remarque.* — Les $\nu$ permutations de ce théorème forment une suite *rentrante* sur elle-même. Car la permutation suivante serait

$$x\ \ x_{p_i\rho^\nu}\ \ x_{2p_i\rho^\nu}\ldots\ x_{(n-1)p_i\rho^\nu},$$

qui n'est autre que la première. Car, en vertu du théorème de Fermat généralisé par Euler, on a

$$\rho^\nu = 1 + \mathrm{M}.n$$

[*] On sait que $\rho$ étant racine *primitive* de $n$, la plus petite puissance de $\rho$ qui soit telle, que $\rho^{k'}-1$ soit divisible par $n$, est le nombre $\nu$ qui marque combien il y a de nombres inférieurs et premiers à $n$.

et par suite

$$kp_i\rho^\nu \equiv kp_i \pmod{n}.$$

Ces polygones étoilés jouissent de plusieurs autres propriétés; mais elles trouveront mieux leur place dans la recherche du nombre de valeurs que peut acquérir une fonction par les permutations des lettres qu'elle renferme ; ce qui précède suffit pour l'intelligence de la classification des permutations qu'offrent $n$ lettres.

## II.

### *Classification des permutations d'un nombre quelconque de lettres.*

*Loi de formation du premier tableau.* — Soient $a$, $b$, $c$,..., $k$, $l$ les lettres que l'on considère en nombre quelconque $n$; le nombre de permutations qu'elles produisent est égal au produit $1.2.3...(n-1).n$.

Parmi ces permutations, prenons toutes celles qui commencent par une même lettre, $a$ par exemple. Pour les obtenir, il suffira de permuter les $n-1$ autres lettres $b$, $c$,..., $k$, $l$ et d'écrire au commencement de chacune d'elles cette lettre $a$. Le nombre de ces permutations ainsi obtenues sera égal au produit $1.2.3...(n-1)$, et elles constituent la *première classe*. Considérons l'une d'elles, $abc...kl$ par exemple, et joignons à cette permutation toutes celles qui sont relatives aux polygones de Poinsot, c'est-à-dire toutes celles qu'on déduit de cette permutation en prenant successivement les lettres, à partir de la première, de $p_1$ en $p_1$, de $p_2$ en $p_2$, etc., et de $p_\nu$ en $p_\nu$, $p_1$, $p_2$,..., $p_\nu$ étant les $\nu$ nombres inférieurs et premiers à $n$. On obtiendra ainsi un premier groupe de $\nu$ permutations, la première comprise,

$$abc...kl,\ adh...ig,\ ....$$

Supprimons ces $\nu$ permutations dans cette première classe et prenons parmi celles qui restent une permutation quelconque, $ahg...ci$ par exemple. Nous ferons sur elle ce que nous avons fait sur la première $abc...kl$, c'est-à-dire que nous prendrons successivement les lettres de cette nouvelle permutation, à partir de la première $a$, de $p_1$ en $p_1$, de $p_2$ en $p_2$, etc., et de $p_\nu$ en $p_\nu$, et nous obtiendrons ainsi un deuxième

groupe de $\nu$ permutations

$$ahg\ldots ci,\quad afl\ldots he,\quad \ldots.$$

Otons encore ces $\nu$ nouvelles permutations de toutes celles que nous avions après la première suppression; prenons parmi celles qui restent une permutation quelconque, $ald\ldots ef$ par exemple, et faisons sur elle ce que nous avons fait sur chacune des deux premières; nous obtiendrons ainsi un troisième groupe de $\nu$ permutations

$$ald\ldots ef,\quad a\ldots,\quad \ldots,$$

et continuons ainsi cette même opération jusqu'à l'entier épuisement des $1.2.3\ldots(n-1)$ permutations de la première classe qui toutes commencent par la même lettre $a$. Cela sera toujours possible, puisque chaque permutation produit $\nu$ permutations seulement et que $\nu$ est un diviseur de ce produit $1.2.3\ldots(n-1)$.

Cette première classe de permutations sera donc décomposée en $\frac{1.2.3\ldots(n-1)}{\nu}$ groupes formés chacun de $\nu$ permutations, ainsi qu'il suit :

$$1^{\text{re}}\text{ classe.}\left\{\begin{array}{l} abc\ldots kl,\quad adh\ldots ig,\ldots,\\ ahg\ldots ci,\quad afl\ldots he,\ldots,\\ ald\ldots ef,\quad a\ldots,\qquad \ldots,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right.$$

On pourrait actuellement prendre les $1.2.3\ldots(n-1)$ permutations des $n$ lettres données qui commencent toutes par une autre lettre, $b$ par exemple, et établir avec elles la même classification qu'on vient de faire sur celles de la première classe. Mais on arrivera évidemment au même résultat, et d'une manière plus simple, si l'on écrit les permutations de cette première classe ligne par ligne et dans le même ordre, en commençant chacune d'elles par cette lettre $b$ et en marchant toujours dans le même sens, de gauche à droite, chaque permutation étant supposée écrite deux fois.

On aura ainsi la deuxième classe de permutations, commençant

toutes par la lettre $b$, partagée en $\frac{1.2.3\ldots(n-1)}{\nu}$ groupes composés chacun de $\nu$ permutations relatives aux $\nu$ polygones de Poinsot :

$$2^e \text{ classe. } \left\{ \begin{array}{l} b\ldots,\ b\ldots,\ \ldots, \\ b\ldots,\ b\ldots,\ \ldots, \\ \ldots\ldots\ldots\ldots\ldots \end{array} \right.$$

De même si l'on écrit les permutations de la première classe, ligne par ligne et dans le même ordre, en commençant chacune d'elles par la lettre $c$ et en marchant toujours de gauche à droite, chaque permutation étant supposée écrite deux fois, on aura une troisième classe de $1.2.3\ldots(n-1)$ permutations commençant toutes par cette lettre $c$ partagée en $\frac{1.2.3\ldots(n-1)}{\nu}$ groupes composés chacun de $\nu$ permutations relatives aux polygones de Poinsot.

En continuant cette même opération jusqu'à l'entier épuisement des $n$ lettres données, toutes les permutations de ces lettres seront distribuées en $n$ classes, et chaque classe en $\frac{1.2.3\ldots(n-1)}{\nu}$ groupes formés chacun de $\nu$ permutations. Telle est la loi de formation du premier tableau.

*Premier tableau.*

$$1^{re} \text{ classe. } \left\{ \begin{array}{lll} abc\ldots kl, & adh\ldots ig, & \ldots, \\ ahg\ldots ci, & afl\ldots he, & \ldots \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots \end{array} \right.$$

$$2^e \text{ classe. } \left\{ \begin{array}{lll} bc\ldots, & b\ldots, & \ldots, \\ b\ldots, & b\ldots, & \ldots, \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots \end{array} \right.$$

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

$$n^{ieme} \text{ classe. } \left\{ \begin{array}{lll} l\ldots, & l\ldots, & \ldots, \\ l\ldots, & l\ldots, & \ldots, \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots \end{array} \right.$$

*Loi de formation du second tableau.* — Prenons les premiers groupes de chacune des $n$ classes du tableau précédent et formons un groupe de ces $n\nu$ permutations

$$abc \ldots kl,\quad adh \ldots ig,\quad \ldots,\quad l \ldots,\quad l \ldots,\quad \ldots.$$

Prenons de même les seconds groupes de chacune des $n$ classes du même tableau et formons un nouveau groupe de ces $n\nu$ permutations

$$ahg \ldots ci,\quad afl \ldots he,\quad \ldots,\quad l \ldots,\quad l \ldots,\quad \ldots.$$

Prenons encore les troisièmes groupes de chacune des mêmes classes; nous en formerons un troisième groupe de $n\nu$ permutations, et continuons cette même série d'opérations jusqu'à ce qu'on ait épuisé les groupes de chaque classe. Nous obtiendrons ainsi un second tableau :

*Second tableau.*

$$\begin{array}{l} abc \ldots kl,\quad adh \ldots ig, \ldots,\quad l \ldots,\quad l \ldots,\quad \ldots, \\ ahg \ldots, ci,\quad afl \ldots he, \ldots,\quad l \ldots,\quad l \ldots,\quad \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

composé d'un nombre de groupes marqué par la formule

$$\frac{1.2.3\ldots(n-1)}{\nu},$$

formés chacun de $n\nu$ permutations assujetties à la même loi, savoir : de $\nu$ permutations relatives aux polygones de Poinsot sur un ordre quelconque des $n$ lettres données, et des $(n-1)\nu$ permutations qu'on déduit de cet ordre en le lisant successivement à partir des lettres $b$, $c, \ldots, l$.

Prenons pour premier exemple $n = 4$, auquel cas $\nu = 2$ et $p_1 = 1$, $p_2 = 3$; le premier tableau sera :

| CLASSE. | ORDRE. | PERMUTATIONS. |
| --- | --- | --- |
| 1 | 1 | *abcd*, *adcb* |
| | 2 | *abdc*, *acdb* |
| | 3 | *adbc*, *acbd* |
| 2 | 4 | *bcda*, *badc* |
| | 5 | *bdca*, *bacd* |
| | 6 | *bcad*, *bdac* |
| 3 | 7 | *cdab*, *cbad* |
| | 8 | *cabd*, *cdba* |
| | 9 | *cadb*, *cbda* |
| 4 | 10 | *dabc*, *dcba* |
| | 11 | *dcab*, *dbac* |
| | 12 | *dbca*, *dacb* |

Le second tableau relatif à ces quatre lettres sera, en désignant par les numéros d'ordre les permutations qui composent les divers groupes dont il se forme :

| ORDRE. | PERMUTATIONS. |
| --- | --- |
| 1 | 1, 4, 7, 10 |
| 2 | 2, 5, 8, 11 |
| 3 | 3, 6, 9, 12 |

Dans cette hypothèse en effet

$$\frac{1.2.3\ldots(n-1)}{\nu} = 3.$$

Prenons pour second et dernier exemple $n = 5$, auquel cas

$$\nu = 4, \quad p_1 = 1, \quad p_2 = 2, \quad p_3 = 3, \quad p_4 = 4 \quad \text{et} \quad \frac{1.2.3\ldots(n-1)}{\nu} = 6:$$

le premier tableau sera :

| CLASSE. | ORDRE. | PERMUTATIONS. |
|---|---|---|
| 1 | 1 | *abcde*, *acebd*, *adbec*, *aedcb*, |
| | 2 | *abced*, *acdbe*, *aebdc*, *adecb*, |
| | 3 | *abecd*, *aedbc*, *acbde*, *adceb*, |
| | 4 | *aebcd*, *abdec*, *acedb*, *adcbe*, |
| | 5 | *abdce*, *adebc*, *acbed*, *aecdb*, |
| | 6 | *adbce*, *abedc*, *acdeb*, *aecbd*, |
| 2 | 7 | *bcdea*, *bdace*, *becad*, *baedc*, |
| | 8 | *bceda*, *beacd*, *bdcae*, *badec*, |
| | .. | ........................ |
| 3 | 13 | *cdeab*, *cebda*, *cadbe*, *cbaed*, |
| | ... | ........................ |
| 4 | 19 | *deabc*, *daceb*, *dbeca*, *dcbae*, |
| | ... | ........................ |
| 5 | 25 | *eabcd*, *ebdac*, *ecadb*, *edcba*, |
| | ... | ........................ |

Le second tableau sera, d'après la notation déjà adoptée :

| ORDRE. | PERMUTATIONS. |
|---|---|
| 1 | 1, 7, 13, 19, 25 |
| 2 | 2, 8, 14, 20, 26 |
| 3 | 3, 9, 15, 21, 27 |
| 4 | 4, 10, 16, 22, 28 |
| 5 | 5, 11, 17, 23, 29 |
| 6 | 6, 12, 18, 24, 30 |

*Propriétés générales des groupes et des classes des deux tableaux précédents.*

THÉORÈME V. — *Les permutations d'un quelconque des groupes du premier tableau sont associées de telle manière, que, malgré tous les échanges qu'on voudrait faire des $n$ lettres qui les forment, elles ne se séparent jamais.*

En effet, plaçons sur une circonférence de rayon arbitraire et à égales distances les unes des autres les $n$ lettres données dans l'ordre qui produit la première des permutations du premier groupe, et formons les $\nu$ polygones réguliers relatifs aux $\nu$ permutations de ce groupe. Le premier polygone s'obtient en joignant les $n$ points désignés par ces lettres un à un, ce qui exige qu'on parcoure une seule fois la circonférence considérée.

Généralement le polygone relatif au nombre inférieur et premier à $n$, $p_i$, s'obtient en joignant les mêmes points de $p_i$ en $p_i$, à partir du point considéré comme origine, ce qui exige qu'on parcoure cette même circonférence $p_i$ fois. Mais, *la théorie de l'ordre étant indépendante de la notion de grandeur,* ce même polygone peut être obtenu en parcourant une *seule* fois une circonférence $p_i$ fois plus grande et en prenant sur elle $n$ points à égale distance les uns des autres, comme pour le premier polygone. Et comme ce résultat est vrai pour toutes les valeurs de $p_i$, $p_1$, $p_2$, $p_3$,..., $p_\nu$, il s'ensuit que les $\nu$ polygones réguliers relatifs au premier groupe du premier tableau ne sont autre chose qu'*un seul et même polygone,* qu'*un seul et même ordre.* Rien ne distingue donc une permutation quelconque de ce groupe d'une autre du même groupe.

Si donc par un échange quelconque de lettres une des permutations de l'un des groupes de ce tableau se change en une autre du même groupe, cet échange ne fera pas sortir de l'*ordre* de ce groupe, et, par suite, toutes les $\nu$ permutations de ce groupe ne feront que s'échanger entre elles, que se déplacer.

Si au contraire un échange quelconque de lettres transformait une des permutations de l'un des groupes du premier tableau en une autre

appartenant à un groupe différent, cet échange ferait passer de l'*ordre* relatif à ce premier groupe à l'*ordre* relatif à ce dernier, et dès lors toutes les permutations de ce premier groupe se changeraient en toutes celles du second. Donc, etc.

THÉORÈME VI. — *Les permutations d'une quelconque des classes du premier tableau sont associées de telle manière, que, malgré tous les échanges qu'on voudrait faire des $n$ lettres qui les forment, elles ne peuvent jamais se séparer.*

Il résulte en effet de la loi de formation du premier tableau et de ce qui vient d'être dit dans la démonstration du théorème précédent, que les permutations de la deuxième classe ayant été obtenues en lisant celles de la première à partir de la lettre $b$, ces permutations ne sont autre chose que *les divers ordres de cette première classe vus d'un autre point*. De même les permutations de la troisième classe ayant été obtenues en lisant celles de la première à partir de la lettre suivante $c$, ces permutations ne sont autre chose que les *divers ordres* de cette première classe vus d'un nouveau point; et ainsi de suite pour les autres classes.

Il suit de là que si un échange de lettres données transforme une permutation d'une des $n$ classes du premier tableau en une autre permutation de la même classe, cet échange ne fera pas sortir du point de vue de cette classe, et que, par suite, les autres permutations de la même classe ne feront que se déplacer par cet échange.

Si, au contraire, un échange des lettres données transformait une des permutations d'une des classes du même tableau en une des permutations d'une autre classe, cet échange ferait passer des divers ordres du point de vue relatif à cette première classe aux divers ordres du point de vue relatif à la seconde, et dès lors toutes les permutations de cette première classe se changeraient en celles de la seconde par suite de cet échange.

THÉORÈME VII. — *Les permutations d'un quelconque des groupes du second tableau sont associées de telle manière, que, malgré tous les échanges qu'on voudrait faire des $n$ lettres qui les forment, elles ne peuvent jamais se séparer.*

En effet, d'après la loi de formation de ces groupes et d'après la démonstration du théorème V, il résulte que l'un quelconque de ces groupes constitue *un seul et même ordre* vu de chacun des $n$ points $a$, $b, \ldots, k, l$. On peut donc appliquer aux groupes de ce second tableau le même raisonnement que celui qu'on vient d'appliquer aux groupes et aux classes du premier. Le théorème VII est donc démontré.

## III.

### *Examen d'un cas particulier.*

Décomposer les permutations de $n$ lettres en plusieurs groupes de permutations *inséparables* quel que soit l'échange de ces lettres, est une idée qui trouve des applications dans la théorie des nombres et dans la théorie générale des équations. C'est même en vue de cette dernière que nous examinerons spécialement le cas où ces $n$ lettres ou choses sont représentées par les $n$ quantités suivantes

$$(1) \qquad x \quad \theta x \quad \theta^2 x \quad \theta^3 x \ldots \quad \theta^{n-1} x,$$

dans lesquelles $x$ désigne l'une quelconque de ces $n$ lettres et $\theta x$ une fonction arbitraire de $x$ telle, que $\theta^n x = x$ : la notation $\theta^2 x$, $\theta^3 x, \ldots$, $\theta^n x$ indiquant qu'il faut répéter deux fois, trois fois,..., $n$ fois les opérations désignées par cette fonction.

Cela posé, nous démontrerons le théorème suivant :

Théorème VIII. — *Cette suite de $n$ fonctions peut être partagée en plusieurs groupes de fonctions* inséparables *quel que soit l'échange des fonctions données : ces groupes eux-mêmes se subdivisent en d'autres groupes de fonctions* inséparables *par l'échange de ces mêmes fonctions; et ainsi de suite pour les groupes successifs obtenus qui se subdivisent d'après* tous *les diviseurs de ce nombre $n$.*

En effet, supposons d'abord $n = \alpha q$. Cette hypothèse permet d'écrire la suite (1) de la manière suivante

$$(2) \qquad x \quad \theta^1(x) \quad \theta^2 x \ldots \quad \theta^{q-1} x \quad \theta^q x \ldots \quad \theta^{2q} x \ldots \quad \theta^{\alpha q-1} x.$$

Actuellement prenons ces fonctions de $q$ en $q$ et successivement à partir de $x$, $\theta x$, $\theta^2 x, \ldots$, $\theta^{q-1} x$, on obtiendra les $q$ groupes suivants composés chacun de $\alpha$ termes :

$$(A) \left\{ \begin{array}{lllll} x & \theta^q x & \theta^{2q} x \ldots & \theta^{(\alpha-1)q}(x), \\ \theta x & \theta^{1+q} x & \theta^{1+2q} x & \theta^{1+(\alpha-1)q} x, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \theta^{q-1} x & \theta^{q-1+q} x & \theta^{q-1+2q} x \ldots & \theta^{q-1+(\alpha-1)q} x. \end{array} \right.$$

Ces $q$ groupes contiennent évidemment les $n$ fonctions de la suite (2) et chacun d'eux est une suite *rentrante* sur elle-même. Ainsi, par exemple, le terme qui suivrait le dernier terme du premier groupe serait $\theta^{\alpha q} x$ ou $\theta^n x$ et $\theta^n x = x$ ; de même le terme qui suivrait le dernier terme du second groupe serait $\theta^{1+q\alpha} x$ ou $\theta^{1+n} x$ ; or $\theta^{1+n} x = \theta x$, puisque $\theta^n x = x$ ; et ainsi de suite pour les autres groupes.

Or si dans l'un de ces groupes, dans le premier par exemple, on change $x$ en $\theta^q x$, le premier terme de ce groupe se change en le second, le second en le troisième, et ainsi de suite, le dernier en le premier ; donc les termes de ce groupe ne font que s'échanger entre eux.

Cet échange produira évidemment le même résultat dans chacun des autres groupes. Il en serait de même si $x$ se changeait en $\theta^{kq} x$, $k$ étant un nombre entier quelconque inférieur à $\alpha$.

Mais si l'on change $x$ en $\theta^2 x$ par exemple, on voit que tous les termes du premier groupe se changent respectivement en ceux du troisième, et qu'ainsi le premier groupe tout entier se substitue au troisième. De même, par cet échange, le second groupe se substitue tout entier au quatrième, et ainsi de suite pour les autres.

Généralement, si l'on change $x$ en $\theta^h x$, $h$ étant plus petit que $\alpha$, il est clair que chacun de ces groupes se substitue tout entier à l'un des groupes du système.

Donc : 1° Si $n = \alpha q$, les termes de la suite (2) peuvent être partagés en $q$ groupes *inséparables* composés chacun de $\alpha$ termes.

Soit de nouveau $q = q' \beta$, auquel cas $n = \alpha\beta q'$.

Si dans le groupe premier du tableau précédent (A) on change $x$ en $\theta x$, on obtient le second. La même transposition change le deuxième

groupe en le troisième, le troisième en le quatrième, etc., et enfin le dernier en le premier. Donc si nous désignons le premier groupe de ce tableau par $F(x)$, les suivants seront successivement désignés par

$$F(\theta x),\ F(\theta^2 x),\ldots,\ F(\theta^{q-1} x)$$

et la suite

$$(3)\qquad F(x),\ F(\theta x),\ F(\theta^2 x),\ \ldots,\ F(\theta^{q-1} x)$$

sera analogue à la suite (2) et comme elle rentrante sur elle-même. Et puisque $q = q'\beta$, on pourra faire sur celle-ci ce qui a été fait sur la première. Donc cette suite (3), et par suite la suite (2), pourra être partagée en $q'$ groupes de termes *inséparables*, quel que soit l'échange des $n$ quantités de la suite (1). Chacun de ces nouveaux groupes sera formé de $\beta$ termes de la suite (3) et par conséquent de $\alpha\beta$ termes de la suite (2).

A nouveau, si l'on suppose encore $q' = q''\gamma$, auquel cas $n = \alpha\beta\gamma q''$, on pourra décomposer les $q'$ groupes de termes obtenus et par conséquent les termes de la suite (2) en $q''$ groupes de termes inséparables, et ainsi de suite.

Comme aussi, en supposant le produit $\alpha\beta\gamma$ effectué, on pourra, d'après le 1°, partager les termes de la suite (2) en $q''$ groupes de termes inséparables composés chacun de $\alpha\beta\gamma$ termes, ou en $\gamma q''$ groupes de termes inséparables composés chacun de $\alpha\beta$ termes, et ainsi de suite pour tous les diviseurs de $n$.

Le théorème énoncé est donc démontré.

*Remarque I.* — Si l'on continue de désigner par $p_1, p_2, p_3, \ldots p_\nu$ les $\nu$ nombres inférieurs et premiers à $n$, on ne peut déduire de la suite (2) que $\nu$ suites composées chacune de tous les termes de cette suite, mais dans un ordre différent, en prenant successivement ces termes à partir du premier $x$ de $p_1$ en $p_1$, de $p_2$ en $p_2$, etc., de $p_\nu$ en $p_\nu$.

Or nous avons démontré dans la deuxième section que ces $\nu$ suites n'étaient autre chose qu'*un seul et même ordre;* donc, en faisant sur chacune d'elles les mêmes opérations qui ont été faites sur la suite (2), on obtiendra exactement les *mêmes* groupes inséparables.

Cette remarque peut être facilement vérifiée sur une valeur particulière, d'ailleurs quelconque, de $n$.

*Remarque II.* — Ce théorème VIII fait retrouver, de la manière la plus simple et la plus élémentaire, comme nous le démontrerons bientôt, tout ce que l'on sait sur les équations binômes et plus généralement sur les équations *abéliennes*.

---

*Addition à la deuxième section.*

Les deux tableaux de permutations relatifs aux cas où $n = 4$ peuvent être suivis d'un troisième jouissant de propriétés analogues.

Si l'on désigne en effet les groupes du premier tableau par les numéros d'ordre qui leur correspondent, le tableau suivant :

| Nos D'ORDRE. | PERMUTATIONS. |
|---|---|
| 1 | 1, 7 |
| 2 | 2, 11 |
| 3 | 3, 6 |
| 4 | 4, 10 |
| 5 | 5, 8 |
| 6 | 9, 12 |

formé de six groupes de permutations composés chacun de quatre permutations, se déduit du premier tableau en joignant à chacun de ses groupes celui qu'on obtient en échangeant 1° les lettres qui occupent la première et la troisième place, 2° celles qui occupent la deuxième et la quatrième.

On constate aisément que les groupes de ce dernier sont également inséparables.

Nous devons encore ajouter que les deux tableaux de permutations

relatifs au cas de trois lettres $a$, $b$, $c$ se réduisent en un seul

$$abc,\ acb,$$
$$bca,\ bac,$$
$$cab,\ cba,$$

mais qu'elles produisent un nouveau tableau de deux groupes de permutations *inséparables* formés chacun de trois permutations

$$abc,\ bca,\ cab,$$
$$acb,\ bac,\ cba,$$

propriété facile à être vérifiée.

## SUR LES DEUX FORMES
## $X^2 + Y^2 + Z^2 + 4T^2, \quad X^2 + 4Y^2 + 4Z^2 + 4T^2$;

PAR M. J. LIOUVILLE.

1. Soit $n$ un nombre entier donné, pair ou impair, que nous représenterons par $2^\alpha m$, $m$ étant impair et l'exposant $\alpha$ pouvant se réduire à zéro. On demande une règle simple qui fasse connaître à priori le nombre N des représentations de $n$, c'est-à-dire le nombre N des solutions de l'équation indéterminée

$$n = X^2 + Y^2 + Z^2 + 4T^2,$$

où X, Y, Z, T sont des entiers quelconques, positifs, nuls ou négatifs.

Après les beaux résultats obtenus par Jacobi concernant la forme

$$x^2 + y^2 + z^2 + t^2,$$

à laquelle est liée intimement celle dont nous venons de parler, la question n'offre pour ainsi dire aucune difficulté.

2. Prenons d'abord $n$ impair, $n = m$, et en désignant par $\zeta_1(m)$ la somme des diviseurs de $m$, nous trouverons

$$N = \left[4 + 2(-1)^{\frac{m-1}{2}}\right]\zeta_1(m),$$

c'est-à-dire

$$N = 6\zeta_1(m)$$

quand $m$ est de la forme $4l + 1$, mais

$$N = 2\zeta_1(m)$$

quand $m$ est de la forme $4l + 3$.

Pour le démontrer supposons d'abord $m = 4l + 1$. Dans l'équation

$$m = x^2 + y^2 + z^2 + t^2,$$

pour laquelle le nombre des solutions est $8\zeta_1(m)$, un des carrés au second membre sera impair, les trois autres pairs. Au lieu d'admettre le carré impair aux quatre places qu'il peut occuper, excluons-le de la dernière et nous diminuerons évidemment dans le rapport de 3 à 4 le nombre des solutions qui deviendra par conséquent $6\zeta_1(m)$. Mais alors $t$ étant pair, $t = 2T$, l'équation

$$m = x^2 + y^2 + z^2 + t^2$$

ne différera pas de la nôtre

$$m = X^2 + Y^2 + Z^2 + 4T^2.$$

Donc, pour nous aussi, il y aura $6\zeta_1(m)$ solutions. L'unité appartient à ce cas de $m$ impair $4l + 1$, et les six représentations qui la concernent sont fournies par les équations que voici :

$$1 = (\pm 1)^2 + 0^2 + 0^2 + 4.0^2,$$
$$1 = 0^2 + (\pm 1)^2 + 0^2 + 4.0^2,$$
$$1 = 0^2 + 0^2 + (\pm 1)^2 + 4.0^2.$$

Soit maintenant $m = 4l + 3$. Le nombre des solutions de l'équation

$$m = x^2 + y^2 + z^2 + t^2$$

continuera à être exprimé par $8\zeta_1(m)$, mais on devra avoir au second membre un seul carré pair et trois carrés impairs, de sorte qu'il ne restera que $2\zeta_1(m)$ solutions si l'on exige que le carré pair soit toujours placé le dernier. Le nombre des solutions de notre équation

$$m = X^2 + Y^2 + Z^2 + 4T^2$$

est donc aussi $2\zeta_1(m)$.

Soit, comme exemple, $m = 3$, d'où $\zeta_1(m) = 4$. On devra trouver huit solutions : elles sont fournies en effet par l'équation

$$3 = (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 + 4.0^2.$$

5. Soit à présent $n$ pair, et d'abord $n$ impairement pair, $n = 2m$. On remarquera que dans l'équation

$$2m = x^2 + y^2 + z^2 + t^2$$

deux des carrés devront être pairs, les deux autres impairs. Les $24\zeta_1(m)$ solutions qu'elle possède d'après le théorème de Jacobi se divisent donc en deux groupes égaux suivant que $t$ est pair ou impair. Ainsi en prenant $t$ pair, $t = 2T$, on n'aura plus que $12\zeta_1(m)$ solutions. Pour le nombre N des solutions de notre équation

$$2m = X^2 + Y^2 + Z^2 + 4T^2,$$

on a donc aussi

$$N = 12\zeta_1(m),$$

quelle que soit la forme linéaire de $m$.

En faisant $m = 1$, on trouve $N = 12$, en sorte que le nombre 2 a douze représentations. Elles sont comprises dans les équations

$$2 = (\pm 1)^2 + (\pm 1)^2 + 0^2 + 4.0^2,$$
$$2 = 0^2 + (\pm 1)^2 + (\pm 1)^2 + 4.0^2,$$
$$2 = (\pm 1)^2 + 0^2 + (\pm 1)^2 + 4.0^2.$$

De même, en faisant $m = 3$, on trouve $N = 48$. Or 6 a en effet quarante-huit représentations que fourniront les deux équations

$$6 = (\pm 1)^2 + (\pm 1)^2 + (\pm 2)^2 + 4.0^2$$

et

$$6 = (\pm 1)^2 + (\pm 1)^2 + 0^2 + 4(\pm 1)^2,$$

si l'on transporte $(\pm 2)^2$ dans l'une, $0^2$ dans l'autre, de la troisième place à la seconde, puis à la première.

4. Pour $n$ divisible par 4, non par 8, $n = 4m$, on remarquera que dans l'équation

$$4m = X^2 + Y^2 + Z^2 + 4T^2,$$

les entiers X, Y, Z ne peuvent être que pairs. On n'altérera donc pas le nombre des solutions en posant, avec $x$, $y$, $z$ entiers,

$$X = 2x, \quad Y = 2y, \quad Z = 2z,$$

de sorte que ce nombre conviendra encore à l'équation

$$m = x^2 + y^2 + z^2 + T^2,$$

pour laquelle on sait d'avance qu'il s'exprime par $8\zeta_1(m)$. Le nombre N des solutions de l'équation

$$4m = X^2 + Y^2 + Z^2 + 8T^2$$

vérifie donc aussi la formule

$$N = 8\zeta_1(m).$$

Le nombre 4, par exemple, doit avoir huit représentations. Les équations qui les fournissent sont

$$4 = (\pm 2)^2 + 0^2 + 0^2 + 4.0^2,$$
$$4 = 0^2 + (\pm 2)^2 + 0^2 + 4.0^2,$$
$$4 = 0^2 + 0^2 + (\pm 2)^2 + 4.0^2,$$
$$4 = 0^2 + 0^2 + 0^2 + 4(\pm 1)^2.$$

5. Soit enfin $n$ divisible par 8, avec quotient pair ou impair, c'est-à-dire soit indifféremment $n = 8m$, $n = 16m$, $n = 32m$, etc. On aura alors pour le nombre N des solutions de l'équation

$$n = X^2 + Y^2 + Z^2 + 4T^2$$

la formule unique

$$N = 24\zeta_1(m).$$

En effet, $n$ étant divisible par 8, posons

$$n = 4.2^{\beta} m$$

et $\beta$ sera $> 0$. Or l'équation

$$4.2^{\beta} m = X^2 + Y^2 + Z^2 + 4T^2$$

ne peut avoir lieu sans que X, Y, Z soient pairs. Nous ferons donc

$$X = 2x, \quad Y = 2y, \quad Z = 2z,$$

et nous en conclurons en nombres entiers l'équation nouvelle

$$2^{\beta} m = x^2 + y^2 + z^2 + T^2,$$

qui devra aussi avoir N solutions. Mais à cause de $\beta > 0$, le nombre des solutions dont elle est susceptible est $24\zeta_1(m)$. Donc

$$N = 24\zeta_1(m),$$

ce qu'il fallait démontrer.

Ainsi pour $n = 8$ et pour $n = 16$, on aura $N = 24$. C'est ce qu'on peut vérifier au moyen des équations respectives

$$8 = 0^2 + 4(\pm 1)^2 + 4(\pm 1)^2 + 4.0^2,$$
$$8 = (\pm 2)^2 + 4(\pm 1)^2 + 4.0^2 + 4.0^2,$$

et

$$16 = 0^2 + 4(\pm 2)^2 + 4.0^2 + 4.0^2,$$
$$16 = (\pm 2)^2 + 4(\pm 1)^2 + 4(\pm 1)^2 + 4(\pm 1)^2,$$
$$16 = (\pm 4)^2 + 4.0^2 + 4.0^2 + 4.0^2,$$

en y effectuant les permutations convenables.

6. Nous venons de déterminer le nombre total N des solutions tant propres qu'impropres de l'équation

$$n = X^2 + Y^2 + Z^2 + 4T^2.$$

On pourrait désirer aussi d'avoir séparément le nombre M des solutions *propres* pour lesquelles aucun entier $> 1$ ne divise à la fois X, Y, Z, T. Alors, au lieu de la fonction numérique $\zeta_1(m)$, il faudra employer avec Eisenstein une autre fonction numérique $Z_1(m)$ qui s'est déjà plusieurs fois présentée à nous. Décomposant l'entier impair $m$ en ses facteurs premiers sous la forme

$$m = a^\mu b^\nu \ldots c^\omega,$$

on a

$$Z_1(m) = (a^\mu + a^{\mu-1})(b^\nu + b^{\nu-1})\ldots(c^\omega + c^{\omega-1}).$$

J'ajoute que nous prenons $Z_1(m) = 1$ pour $m = 1$.

Cela étant, voici les diverses valeurs de M relativement aux cas à distinguer dans l'équation

$$n = 2^\alpha m.$$

Pour $n$ impair, $n = m$, on a

$$M = 6 Z_1(m)$$

quand $m$ est de la forme $4l + 1$, mais

$$M = 2 Z_1(m)$$

quand $m$ est de la forme $4l + 3$.

Pour $n$ impairement pair, $n = 2m$, on a

$$M = 12 Z_1(m).$$

Pour $n$ divisible par 4, non par 8, $n = 4m$, on a

$$M = 2 Z_1(m)$$

quand $m$ est de la forme $4l + 1$, mais

$$M = 6 Z_1(m)$$

quand $m$ est de la forme $4l + 3$, de sorte qu'il se produit une sorte d'inversion dans les coefficients qui s'étaient présentés lorsqu'on avait $n = m$.

Pour $n$ divisible par 8, non par 16, $n = 8m$, on a

$$M = 12 Z_1(m).$$

Pour $n$ divisible par 16, non par 32, $n = 16m$, on a

$$M = 16 Z_1(m).$$

Enfin pour $m$ divisible par 32, avec quotient pair ou impair, il vient généralement

$$M = 0.$$

Il n'y a donc plus alors de solutions propres. On verra facilement à priori qu'il en doit être ainsi, les entiers X, Y, Z, T ne pouvant manquer d'être dans ce cas tous divisibles par 2.

7. Ce qui concerne la représentation d'un entier donné $n = 2^\alpha m$, par la forme

$$X^2 + 4Y^2 + 4Z^2 + 4T^2,$$

est tout aussi simple.

Cherchons, en premier lieu, le nombre total Q des représentations tant propres qu'impropres, et nous verrons d'abord que pour $n$ impair, $n = m$, on a $Q = 0$, si $m = 4l + 3$; mais si, au contraire, $m = 4l + 1$, il vient

$$Q = 2\zeta_1(m),$$

car l'équation

$$4l + 1 = X^2 + 4Y^2 + 4X^2 + 4Z^2$$

ne diffère de celle de Jacobi

$$4l + 1 = x^2 + y^2 + z^2 + t^2,$$

que par la place assignée au carré impair $X^2$.

Pour $n$ impairement pair, $n = 2m$, on retrouve

$$Q = 0,$$

quelle que soit la forme linéaire de $m$.

Pour $n$ divisible par 4, non par 8, $n = 4m$, on obtient

$$Q = 8\zeta_1(m),$$

car l'équation

$$4m = X^2 + 4Y^2 + 4Z^2 + 4T^2,$$

où l'on a nécessairement X pair $= 2x$, se ramène à celle-ci :

$$m = x^2 + Y^2 + Z^2 + T^2.$$

Semblablement pour $n$ divisible par 8, que le quotient soit pair ou impair, on a toujours

$$Q = 24\zeta_1(m).$$

Quant au nombre P des représentations propres, il dépend de la fonction $Z_1(m)$.

Soit d'abord $n$ impair, $n = m$, on aura

$$P = 0,$$

si $m = 4l + 3$; mais

$$P = 2Z_1(m),$$

si $m = 4l + 1$.

Pour $n$ impairement pair, $n = 2m$, on a au contraire

$$P = 0,$$

quelle que soit la forme linéaire de $m$.

Pour $n$ divisible par 4, non par 8, $n = 4m$, il faut de nouveau distinguer deux cas. On a, en effet,

$$P = 8Z_1(m)$$

quand $m = 4l + 3$, mais

$$P = 6Z_1(m)$$

quand $m = 4l + 1$.

Pour $n$ divisible par 8, non par 16, $n = 8m$, il vient l'équation unique

$$P = 24Z_1(m),$$

quelle que soit la forme linéaire de $m$.

De même, pour $n$ divisible par 16, non par 32, $n = 16m$, on a

$$P = 16 Z_1(m).$$

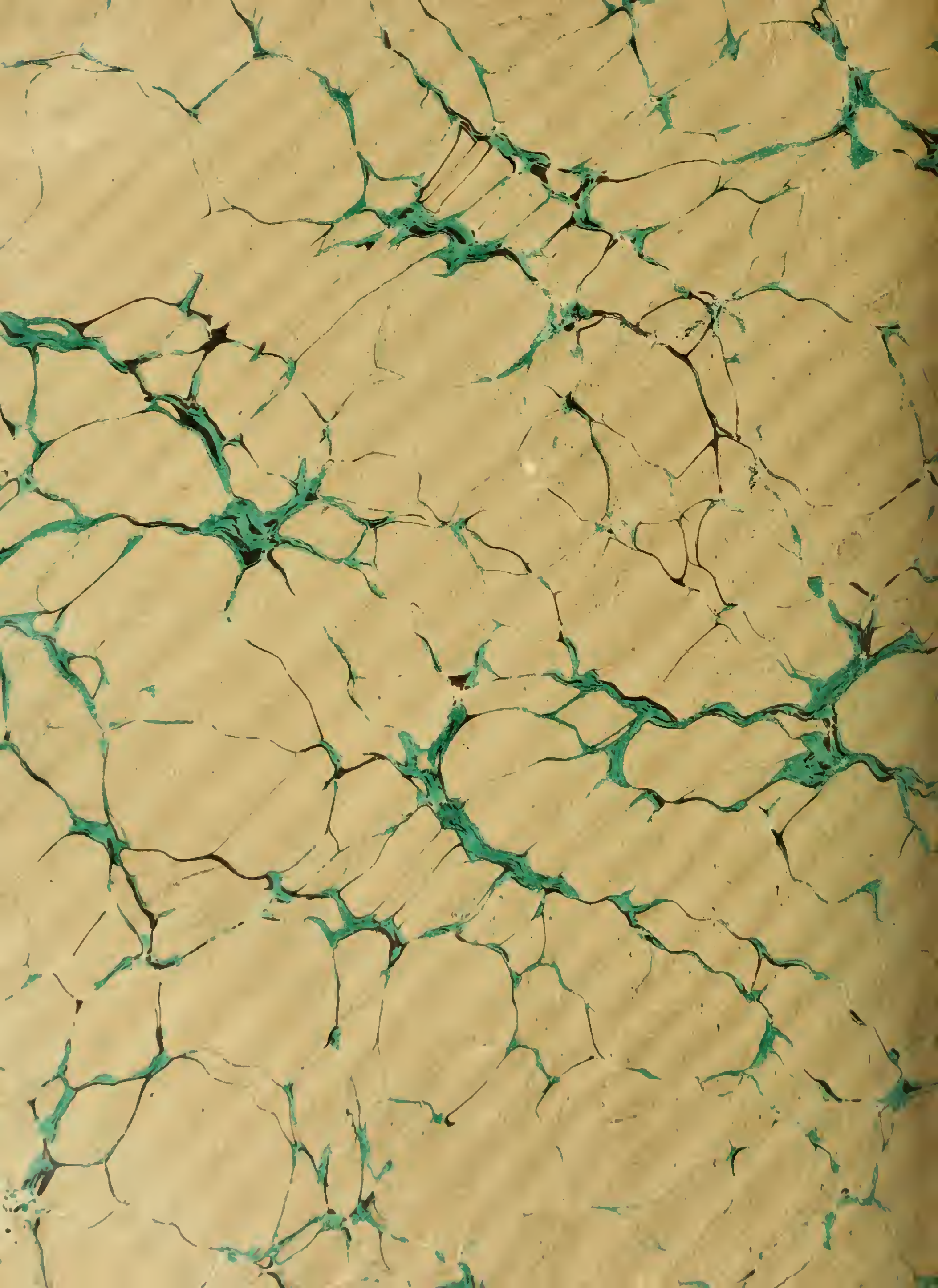
Au delà il n'y a plus de représentations propres, en sorte que pour $n$ divisible par 32, quel que soit le quotient, on a toujours

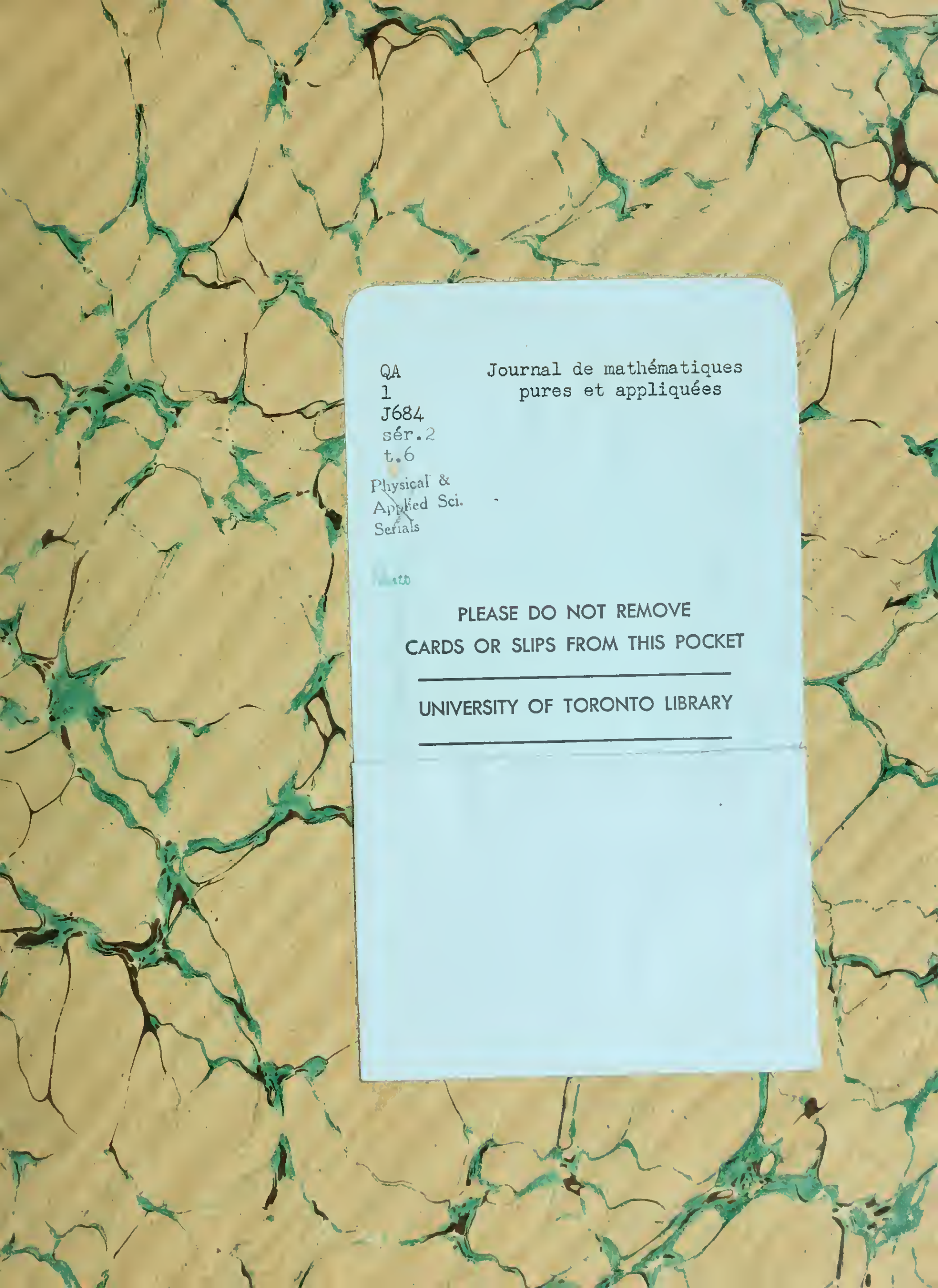
$$P = 0.$$

Cela est, du reste, évident à priori.

FIN DU TOME SIXIÈME (2^e SÉRIE).

PARIS. — IMPRIMERIE DE MALLET-BACHELIER,
rue de Seine-Saint-Germain, 10, près l'Institut.





QA
1
J684
sér.2
t.6
Physical &
Applied Sci.
Serials
Journal de mathématiques
pures et appliquées
PLEASE DO NOT REMOVE
CARDS OR SLIPS FROM THIS POCKET
UNIVERSITY OF TORONTO LIBRARY